UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	Civil Action No. 2:17-cv-00383/HCM-LRL
	)	
v.	)	
	)	
KEYSIGHT TECHNOLOGIES, INC., and IXIA,	)	
	)	
	)	
Defendants	)	

REPORT OF ADAM SORINI REGARDING INVALIDITY OF U.S. PATENT NOS. 9,137,205, 9,264,370, 9,413,722, 9,565,213, 9,917,856, AND 9,560,077.

Table of Contents

I. SCOPE 4
II. INTRODUCTION 5
III. EXPERIENCE 6
IV. LEGAL UNDERSTANDING 10
1. Prior Art 10
2. Anticipation 11
3. Obviousness 11
4. Written Description and Enablement 13
V. PERSON OF ORDINARY SKILL IN THE ART 14
VI. CLAIM CONSTRUCTION 14
VII. TECHNOLOGY BACKGROUND 19
VIII. PRIOR ART BACKGROUND 22
IX. THE ACCUSED PRODUCTS 23
A. NTO 5236 AND NTO 5236 WITH ADVANCED FEATURE MODULE 23
X. U.S. PATENT NO. 9,137,205 28
B. SUMMARY OF THE '205 PATENT 28
C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF TIPPINGPOINT IPS 31
1. TEST CONFIGURATION WITH TIPPINGPOINT IPS 33
2. CLAIM 17 37
3. CLAIM 33 63
D. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF CHECK POINT R75 67
1. TEST CONFIGURATION WITH CHECK POINT R75 70
2. CLAIM 17 73
3. CLAIM 33 99
E. OBVIOUSNESS IN VIEW OF US PATENT NO. 8,955,128 IN COMBINATION WITH POLIWALL AND NTO 5236 103
1. US PATENT NO. 8,955,128 103
2. POLIWALL 105
3. NTO 5236 108
4. NTO 5200 User Guide 110
5. MOTIVATION TO COMBINE 111
6. CLAIM 17 113
7. CLAIM 33 124

XI. U.S. PATENT NO. 9,264,370 127
XII. U.S. PATENT NO. 9,413,722 128
A. SUMMARY OF THE '722 PATENT 128
B. THE ASSERTED SUBJECT MATTER OF THE '722 PATENT 131
C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF TIPPINGPOINT IPS ... 132
1. TEST CONFIGURATION WITH TIPPINGPOINT IPS 133
2. CLAIM 1 137
3. CLAIM 25 160
D. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF CHECK POINT R77 ... 165
1. TEST CONFIGURATION WITH CHECK POINT R77 167
2. CLAIM 1 169
3. CLAIM 25 196
E. OBVIOUSNESS IN VIEW OF US PATENT NO. 8,955,128 IN COMBINATION WITH POLIWALL AND NTO 7300 201
1. US PATENT NO. 8,955,128 201
2. POLIWALL 203
3. NTO 7300 204
4. MOTIVATION TO COMBINE 207
5. CLAIM 1 209
6. CLAIM 25 221
XIII. U.S. PATENT NO. 9,565,213 222
A. SUMMARY OF THE '213 PATENT 222
B. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF TIPPINGPOINT IPS ... 226
1. TEST CONFIGURATION WITH TIPPINGPOINT IPS 227
2. CLAIM 1 230
3. CLAIM 3 255
C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF CHECK POINT R75 ... 256
1. TEST CONFIGURATION WITH CHECK POINT R75 257
2. CLAIM 1 259
3. CLAIM 3 284
XIV. U.S. PATENT NO. 9,917,856 284
A. SUMMARY OF THE '856 PATENT 285
B. ANTICIPATION IN VIEW OF CHECK POINT R77 288
1. TEST CONFIGURATION WITH CHECK POINT R77 289
2. CLAIM 1 290

3. CLAIM 18 315
4. CLAIM 24 317
5. CLAIM 25 321
C. OBVIOUSNESS IN VIEW OF BLUE COAT IN COMBINATION WITH TIPPING POINT IPS 325
1. BLUE COAT IN COMBINATION WITH TIPPING POINT 325
2. MOTIVATION TO COMBINE 327
3. CLAIM 1 329
4. CLAIM 18 342
5. CLAIM 24 344
6. CLAIM 25 347
XV. U.S. PATENT NO. 9,560,077 351
A. SUMMARY OF THE '077 PATENT 351
B. ANTICIPATION BY NTO 5236 355
1. NTO 5236 355
2. NTO 5200 User Guide 357
3. CLAIM 7 358
4. CLAIM 13 362
C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF NTO 5236 AND TIPPINGPOINT IPS 362
D. LACK OF WRITTEN DESCRIPTION 363
XVI. DECLARATION 368

I. SCOPE

1. At the request of Keysight Technologies Inc ("Keysight") and IXIA, Exponent provided technical services and opinions relating to the matter of Centripetal Networks, Inc., v. Keysight Technologies, Inc., and IXIA, associated with U.S. Patent No. 9,137,205, U.S. Patent No. 9,413,722, U.S. Patent No. 9,565,213, U.S. Patent No. 9,917,856, and U.S. Patent No. 9,560,077. Exponent investigated specific issues relevant to this matter as requested by the client. The

opinions and comments formulated during this assessment are based on observations and information available at the time of the investigation.

2. The findings presented herein are made to a reasonable degree of scientific certainty. I have made every effort to accurately and completely investigate all areas of concern identified during our investigation. I reserve the right to supplement this report if and when new information becomes available after this report is signed, including, but not limited to, additional discovery or documents, opinions of the court, and the opinions and testimony of other experts in this case. I also reserve the right to respond to any opinions offered by other experts and to any testimony offered at trial. And, I also reserve the right to create graphics or demonstratives to support my opinions at trial.

II. INTRODUCTION

3. I, Adam Sorini, am currently a Senior Managing Scientist at Exponent, Inc. ("Exponent"), an engineering and scientific consulting firm headquartered at 149 Commonwealth Drive, Menlo Park, CA 94025. I am based in Exponent's Menlo Park office, and I am part of Exponent's Electrical Engineering and Computer Science (EECS) practice.

4. Exponent was retained by Keysight to provide technical services and opinions in the matter Centripetal Networks, Inc., v. Keysight Technologies, Inc., and IXIA, Civil Action No. 2:17-cv-00383/HCM-LRL in the United States District Court for the Eastern District of Virginia, Norfolk Division ("Centripetal v. Keysight").

5. I am a salaried employee of Exponent. Exponent charges an hourly rate of $320 plus expenses for my work performed in connection with this matter. I have received no additional compensation for my work in this matter, and my compensation does not depend upon the contents of this report, any testimony I may provide, or the ultimate outcome of this litigation.

III. EXPERIENCE

6. I have worked in Exponent's EECS practice for more than six years. Prior to joining Exponent, I worked as a post-doctoral researcher at the Lawrence Livermore National Laboratory (LLNL), which is a multi-program national security laboratory sponsored primarily by the National Nuclear Security Administration, within the U.S. Department of Energy (DOE). At LLNL I worked on large-scale computational physics research, including DOE classified research, which required a Q-type clearance (similar to Department of Defense "Top Secret"). I also worked as a post-doctoral research at Stanford University, where I developed computer software to study electronic systems.

7. At Exponent, I have been involved with numerous computer security matters involving servers, desktop computers, laptops, tablets, smartphone, and embedded systems. For example, I have investigated cyber-attacks (e.g., ransomware) on large organizations with hundreds of servers.

8. I have also been involved in the architecture and implementation of computer security systems for medical devices. I have also inspected a variety of web applications for security issues. Systems that I have designed and implemented as part of my work at Exponent make use of modern authenticated encryption protocols as well as modern cryptographic hash-based integrity protocols. I have also implemented security functionality such as AES256 symmetric encryption and SHA256-based HMAC functionality on microcontroller devices. I have also setup and utilized asymmetric encryption protocols such as RSA for use with web application security. In addition to design and implementation, I have also reviewed the software and firmware of network connected devices to discover and mitigate security vulnerabilities.

9. I also have experience with analysis of large source code repositories, including source code security analysis. I also have experience in reverse engineering of compiled software applications to understand, for example, functionality involved in the circumvention of software security systems.

10. In addition, I also have extensive experience in the field of digital forensics and have investigated and analyzed network artifacts such as SMTP headers, Windows SMB Protocol information, HTTP and HTTPS headers, as well as other application layer data. In my work, I also routinely deal with lower layer protocols such as TCP, IP, Wi-Fi, Ethernet, Bluetooth, I^2C, and others. I have also collected, preserved, and analyzed data from a wide variety of storage devices such as disk drives, SD cards, and USB thumb drives and a wide variety of file systems such as FAT, ext, and NTFS.

11. I have authored 30 articles (the majority in peer-reviewed publications) and numerous conference presentations in the field of electronic systems, computer and smart phone forensics, and cybersecurity.

12. Additionally, I am a Certified Cyber-Forensics Professional (CCFP) as recognized by the International Information System Security Certification Consortium (ISC2). I am also a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). A copy of my CV is attached hereto as Exhibit A.

13. My opinions, as expressed in this report, are based on my education, career, and relevant experience, as well as the materials I reviewed for this matter. These materials include, but are not limited to, the documents listed in Table 1 below.

Table 1: List of Materials Reviewed

Materials Reviewed
U.S. Patent No. 9,137,205 ("the '205 Patent")

Materials Reviewed
U.S. Patent No. 9,413,722 ("the '722 Patent")
U.S. Patent No. 9,560,077 ("the '077 Patent")
U.S. Patent No. 9,917,856 ("the '856 Patent")
U.S. Patent No. 9,565,213 ("the '213 Patent")
Centripetal Networks, Inc.'s Second Supplemental Responses to Defendants' Interrogatory No. 5 and attached Exhibits: A, B1, B2, C1, C2, D1, D2.
Centripetal Networks, Inc.'s Third Supplemental Responses to Defendants' Interrogatory No. 5
Centripetal Networks, Inc.'s Fourth Supplemental Responses to Defendants' Interrogatory No. 5 and attached Exhibits: E1, E1 (corrected), E2, and F
Plaintiff Centripetal Networks, Inc.'s Identification of Asserted Claims
Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))
Defendant Keysight Technologies, Inc. And Ixia's Identification of Prior Art
CheckPoint R75 documentation[1]
TippingPoint Unity One 200 manual[2]
CheckPoint R77.20 documentation[3]
Poliwall manual (BAND-TGS00250-0346)
Additional Poliwall documentation (including PA0005443.pdf , and PA0005453.pdf, 140sp1879.pdf, and BAND-TGS00468-487)
Poliwall video 1 (https://www.youtube.com/watch?v=z62og8lNk5A)
US PATENT 8,955,128 (Trama)
US PATENT 5,835,726 (Shwed)
US PATENT 7,454,792 (Cantrell)
NTO 7300 Manual[4]
Bluecoat documentation[5]

[1] The CheckPoint R75 documentation includes such documents as: "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010); "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010); and "R75 Installation and Upgrade Guide" (dated Dec 15, 2010).
[2] The TippingPoint Unity One 200 manual includes such documents as: "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) and "TippingPoint IPS Hardware Installation and Safety Guide v 2.5.4" (copyright 2008).
[3] The CheckPoint R77.20 documentation includes such documents as: "Check Point R77 Firewall Administration Guide" (dated Aug 27, 2013) and "Check Point R77 Security Management Server Administration Guide" (dated Aug 27, 2013).
[4] "Anue Net Tool Optimizer 7300 Series User Guide" (dated 2014)

Materials Reviewed
US PATENT Application 2012/0304244 (Xie)
US PATENT Application 2008/0072307 (Maes)
US PATENT 8,438,270 (Nappier)
US PATENT 9,419,942 (Buruganahalli)
US PATENT 7,185,365 (Tang)
US PATENT Application 2009/0216875 (Shi)
OpenFlow Switch Specification, Version 1.1.0 (PA0013163.pdf)
US PATENT 8,954,957 (Wu)
US PATENT Application 2007/0147380 (Ormazabal)
Anue 5200 Manual[6]
DEFENDANT IXIA'S RESPONSES TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S FIRST SET OF INTERROGATORIES (NOS. 1-14)
DEFENDANT KEYSIGHT'S RESPONSES TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S FIRST SET OF INTERROGATORIES TO (NOS. 1-16) and attached Exhibit
DEFENDANT IXIA'S THIRD SUPPLEMENTAL RESPONSE TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S INTERROGATORY NO. 2 and attached Exhibits
DEFENDANT KEYSIGHT'S THIRD SUPPLEMENTAL RESPONSE TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S INTERROGATORY NO. 2 and attached Exhibits
DEFENDANT IXIA'S SECOND SUPPLEMENTAL RESPONSE TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S INTERROGATORY NO. 2 and attached Exhibits
DEFENDANT KEYSIGHT'S FIRST SUPPLEMENTAL RESPONSES TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S INTERROGATORY NOS. 2, 9 AND SECOND SUPPLEMENTAL RESPONSES TO INTERROGATORY NOS. 15-16 and attached Exhibits
DEFENDANT IXIA'S FIRST SUPPLEMENTAL RESPONSE TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S INTERROGATORY NOS. 2, 8, 11-12 and attached Exhibits

[5] Including documents: "140sp2361.pdf"; "bcs_sb_SSL_Visibility_EN_v1c.pdf"; "bcs_sb_Top7_Reasons_Deploy_SSLVisibility_EN_v1b.pdf"; "bcs_wp_5Steps_for_Stronger_Advanced_Threat_Protection_EN_v2b.pdf"; "bcs_wp_Accelerate_SSL_Encrypted_Applications_EN_5b.pdf.pdf"; "Blue-Coat-and-SafeNet-Luna-SB-(EN)-v3-Apr142015-web.pdf"; "dg-blue-coat-and-fireeye-with-gigamon.pdf"; "encrypted-traffic-management-for-dummies-en.pdf"; "SV2800_SV3800_GettingStartedGuide_3.8.pdf"; "US8225085.pdf"; "US8813189.pdf"; "Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide" (dated 9/22/2014); "Blue Coat SSL Visibility SV800 and SV1800 Getting Started Guide" (dated 09/19/2014).

[6] "Anue Net Tool Optimizer 5200 Series User Guide" (dated 2013)

Materials Reviewed
DEFENDANT IXIA'S RESPONSES TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S FIRST SET OF INTERROGATORIES (NOS. 1-14) and attached Exhibits
DEFENDANT KEYSIGHT'S RESPONSES TO PLAINTIFF CENTRIPETAL NETWORKS, INC.'S FIRST SET OF INTERROGATORIES TO (NOS. 1-16) and attached Exhibits
EXPERT REPORT OF DR. ERIC COLE REGARDING INFRINGEMENT BY KEYSIGHT TECHNOLOGIES, INC. AND IXIA OF PATENT NOS. 9,264,370, 9,917,856 and 9,413,722 and attached Exhibit and Appendix
EXPERT REPORT OF MICHAEL GOODRICH, PH.D. REGARDING THE TECHNOLOGY OF U.S. PATENT NOS. 9,137,205; 9,560,077; 9,565,213; 9,264,370; 9,413,722 AND 9,917,856 AND THE ACCUSED TECHNOLOGIES and attached Appendices
EXPERT REPORT OF NENAD MEDVIDOVIĆ, PH.D. REGARDING TECHNOLOGY TUTORIAL AND TECHNOLOGY OF U.S. PATENT NOS. 9,137,205; 9,560,077; 9,565,213; 9,264,370; 9,413,722 AND 9,917,856 and attached Appendices
EXPERT REPORT OF DR. MICHAEL MITZENMACHER REGARDING INFRINGEMENT BY KEYSIGHT TECHNOLOGIES, INC. AND IXIA OF PATENT NOS. 9,137,205; 9,560, 077; AND 9,565,213 and attached Appendices
EXPERT REPORT OF DR. RICARDO VALERDI REGARDING COST ESTIMATES and Attachments
EXPERT REPORT OF WILLIAM G. KRIEGER and attached Appendices and Exhibits
7300 User Guide
Vision ONE User Guide
Deposition Transcripts of David E. Maestras (dated July 26, 2018)
Declaration of Dario David In Support of Defendants' Motion for Summary Judgement of Invalidity (dated May 25, 2018)
Declaration of Gene Munson In Support Of Defendants' Motion for Summary Judgement of Invalidity (dated May 24, 2018)
Opinion & Order of Judge Henry Coke Morgan, Jr. dated November 15, 2017 (Dkt. 53)

IV. LEGAL UNDERSTANDING

1. Prior Art

14. I have been informed by counsel that prior art includes various categories of information such as printed publications, patents, actual commercial products and/or other physical

embodiments. I also have been informed by counsel and generally understand that a patent, publication, or product qualifies as prior art to a challenged claim if it was issued, published, or sold more than a year before the priority date of the patent containing the challenged claim. I have also been informed that, starting in 2013, the grace period of one year prior to the filing date does not necessarily apply. I also understand that a patent or published patent application can qualify as prior art if it was filed before the invention claimed in the challenged patent.

2. Anticipation

15. I have been informed by counsel and generally understand that a patent claim is invalid for anticipation when a single prior art reference teaches each and every element of the claim as arranged in the claim. I further understand from counsel that each element may be expressly or inherently contained within a single prior art reference in order for it to anticipate. I have been informed that for an element to be inherently disclosed, that one of ordinary skill in the art must understand that the missing element must necessarily be present in the prior art reference.

3. Obviousness

16. I have been informed by counsel and generally understand that a patent claim is invalid if a person of ordinary skill in the art at the time of the alleged invention would have found the invention obvious in light of one or more prior art references. I understand from counsel that to make a determination that a claim is obvious, the Court must consider (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of one of ordinary skill in the art; and (4) objective evidence that may weigh against a finding of obviousness. I understand from counsel that objective evidence (so

called, secondary considerations) can include, among other things, commercial success of the claimed invention, a long felt need for the claimed invention failure of others, copying of the invention by others, and praise by others.

17. I further understand from counsel that when modifying a reference or combining references for an obviousness analysis, there must be an apparent reason to do so with a rational underpinning, and there must be some expectation of success. Counsel has informed me that hindsight analysis is to be avoided, and each reference must be considered in its entirety, including portions which may tend to teach away from the proposed modification or combination. I note that, to date, I have not seen any evidence of "secondary considerations" for the patent claims discussed herein that would change my ultimate conclusions of obviousness, where applicable.

18. Counsel has also informed me that a conclusion of obviousness may be found where, for example, the invention is nothing more than (1) a combination of prior art elements according to known methods to yield predictable results; (2) a simple substitution of one known element for another to obtain predictable results; (3) the use of a known technique to improve similar devices in the same way; or (4) the application of a known technique to a known device ready for improvement to yield predictable results. I also understand from counsel that an invention may be obvious if it would have been obvious to try, i.e., selecting from a finite number of identified, predictable solutions with a reasonable expectation of success. I am also informed by counsel that an invention may be obvious is there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify a prior art reference or combine prior art teachings to arrive at the claimed invention. This inquiry poses the question as to whether there is an explicit

teaching, suggestion, or motivation in the prior art to combine prior art elements in a way that realizes the claimed invention. Though useful to the obviousness inquiry, I understand that this inquiry should not be treated as a rigid rule. It is not necessary to seek out precise teachings, but is permissible to consider the inferences and conclusions that would be drawn by one of ordinary skill in the art.

4. Written Description and Enablement

19. Counsel has also informed me a patent may be deemed invalid if it fails to contain a written description of the invention that is sufficient to convey to one of ordinary skill in the art that the inventor had possession of the claimed invention at the time the inventor filed for his patent. I understand this to be legally referred to as the "written description" requirement.

20. Counsel has also informed me that the patent specification must teach one of ordinary skill in the art, at the time the patent application was filed, how to make and use the full scope of the claimed invention without undue experimentation. I understand this to be legally referred to as the "enablement" requirement. When considering the issue of enablement, I understand that I should also consider the so-called "Wands factors", which include the following:

- The breadth of the claims;
- The nature of the invention;
- The state of the prior art;
- The level of one of ordinary skill;
- The level of predictability in the art;
- The amount of direction provided by the inventor;
- The existence of working examples; and
- The quantity of experimentation needed to make or use the invention based on the content of the disclosure.

V. PERSON OF ORDINARY SKILL IN THE ART

21. It is my understanding that patent claims should be understood from the perspective of a person of ordinary skill in the art ("POSITA") to which the patents relate, and based on the understanding of said POSITA at the priority of the relevant patent. Due to the similar nature of the underlying technology, descriptions within the specifications, and claimed material, it is my opinion that the same level of experience and skill is applicable to a POSITA for all the patents-in-suit. Although I have applied the same level of experience and skill to the POSITA for all patents-in-suit, I have done so while considering the different priority dates such that the POSITA for a given patent is appropriate for the particular priority date of said patent.

22. In my opinion, a POSITA for the '077 Patent, the '205 Patent, the '213 Patent, the '722 Patent, and the '865 Patent would be: (1) a person with a Bachelor of Science degree, or its equivalent, in electrical engineering, computer engineering, computer science, or a related field; or (2) a person with a certification in cybersecurity and approximately two years of related experience in the field of network security or cybersecurity.

VI. CLAIM CONSTRUCTION

23. Exhibit 1 of the Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL)) contains a chart noting the claim terms with constructions to which the parties have agreed upon. These constructions are listed in Table 2 through Table 4 below, according to the patent to which they apply.

Term	Agreed Construction
packet security gateway	a gateway computer configured to receive packets and perform a packet transformation function on the packets
security policy management server	a server configured to manage policies and communicate a dynamic security policy to a packet security gateway

Table 2. Agreed upon constructions for claim terms of the '205 Patent

Term	Agreed Construction
LAN switch	a network device configured to send and receive data between computers on a local area network
network-layer address	an address that identifies a device for communication on the network layer, such as an IP address

Table 3. Agreed upon constructions for claim terms of the '077 Patent

Term	Agreed Construction
network-threat indicators	indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like

Table 4. Agreed upon constructions for claim terms of the '722 Patent

Term	Agreed Construction
packet security gateway	gateway computer configured to receive packets and perform a packet transformation function on the packets
security policy management server	a server configured to manage policies and communicate a dynamic security policy to a packet security gateway
packet digest logging function	a function that identifies a subset of information for a packet and generates a record
logging system standard	a standard for logging information
application-layer packet-header information	information in the header of a packet that corresponds to the application-layer

Table 5. Agreed upon constructions for claim terms of the '213 Patent

Term	Agreed Construction
network-threat indicators	indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like
handshake messages	messages to establish a session or connection

Table 6. Agreed upon constructions for claim terms of the '856 Patent

24. I have applied these constructions throughout my analysis.

25. Exhibit 2 of the Joint Claim Construction and Prehearing Statement contains a chart noting the parties' respective proposed constructions of disputed claim terms. These terms and disputed constructions are listed in Table 7 through Table 9 below, according to the patent to which they apply.

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
packet transformation function/functions	function that transforms one or more packets from one state to another	an operation performed on a packet specified by the dynamic security policy, such as forward or drop
dynamic security policy/policies	a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets	any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria
rule/rules	condition or set of conditions that when satisfied cause a specific action to occur	(i) packet-identifying criteria and (ii) a function to be performed on the identified packets

Table 7. Parties' proposed constructions of disputed claim terms of the '205 Patent

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
rule/rules	condition or set of conditions that when satisfied cause a specific action to occur	(i) packet-identifying criteria and (ii) a function to be performed on the identified packets
switching matrix of local area network (LAN) switch	a matrix contained within a local area network switch that may be configured to direct traffic from one device to another device in the network	a structure configured to switch packets received from one or more devices on a local area network to one or more devices on the local area network
provision/provisioning each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located	change a device from one state to another based on one or more rules derived from the boundary of a different network	no construction needed/plain meaning
subscription service	service that provides aggregated	service that aggregates

	information related to malicious network traffic	information associated with malicious network traffic

Table 8. Parties' proposed constructions of disputed claim terms of the '077 Patent

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
packet-filtering device	a device programmed to filter packets based on data associated with a packet	no construction needed/plain meaning
packet-filtering rules	condition or set of conditions that when satisfied cause a computing device to filter packets based on data associated with a packet	(i) packet-identifying criteria and (ii) an operator to be performed on the identified packets
interface	plain and ordinary meaning	a display visible to the user that allows a user to provide input
operator	an adjustable instruction that causes the packet filtering device to either prevent or allow a packet to continue to a destination"	function to either prevent a packet corresponding to criteria from continuing or allow it to continue to its destination
responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators	if the packet-filtering device determines the first packet meets one or more conditions associated with one or more network threat indicators from a packet filtering rule	no construction needed/plain meaning
communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet	causing a packet-filtering device to generate and communicate a record that identifies (1) a network threat indicator based on a rule and (2) data that indicates that the first packet was allowed to continue toward the destination	no construction needed/plain meaning
modifying, by the	modifying the state of the packet-	no construction needed/plain

packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations	filtering device to cause an adjustable instruction to prevent a packet from continuing toward its destination	meaning
user	plain and ordinary meaning	person (e.g., administrator)

Table 9. Parties' proposed constructions of disputed claim terms of the '722 Patent

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
packet transformation function/functions	function that transforms one or more packets from one state to another	an operation performed on a packet specified by the dynamic security policy, such as forward or drop
dynamic security policy/policies	a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets	any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria

Table 10. Parties' proposed constructions of disputed claim terms of the '213 Patent

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
packet-filtering rules	condition or set of conditions that when satisfied cause a computing device to filter packets based on data associated with a packet	(i) packet-identifying criteria and (ii) an operator to be performed on the identified packets
proxy system	plain and ordinary meaning	system that establishes connections to devices in trusted and untrusted environments and relays packets between a device in the trusted environment and a device in the untrusted environment

Table 11. Parties' proposed constructions of disputed claim terms of the '856 Patent

26. I understand that the Court will not rule upon the construction of the disputed claims until after this report must be submitted, and thus I have considered both the proposed constructions of the relevant claim terms in rendering my opinions.

VII. TECHNOLOGY BACKGROUND

27. The patents-in-suit are related to packet filtering of network traffic, and claim various specific systems and methods by which packet filtering may be implemented.

28. Since as early as the 1980s[7], and up to the present day, computer networks have transferred information in packets using the ubiquitous TCP/IP protocol. The TCP/IP protocol has been a public standard for Internet communication since the birth of commercially available Internet services in the 1990's.[8]

29. Computer networking is conventionally divided into layers which provide increasingly abstracted functions with the lowest being the hardware or physical layer and the highest being the application layer.[9]

30. The application layer includes protocols such as HTTP, FTP, SMTP, as so on. These protocols allow applications to communication over networks. For example, a web client and a web server can communicate over the Internet using the HTTP protocol. The web client makes HTTP requests such as "GET / HTTP/1.1" and the web server sends responses such as "HTTP/1.1 200 OK" (as well as the requested data if applicable). HTTP requests and responses can also include metadata called "headers," which can be made up of colon-separated key/value pairs. For example, the web client may include a HTTP header indicating that the "User-Agent"

---

[7] Kurose J. F. and Ross K. W., "Computer Networking: A Top-Down Approach," Fifth Edition (2010) at Section 1.7.3, page 65: "January 1, 1983 saw the official deployment of TCP/IP as the new standard host protocol for ARPAnet."

[8] http://www.computerhistory.org/timeline/networking-the-web/

[9] See, for example, Kurose J. F. and Ross K. W., "Computer Networking: A Top-Down Approach," Fifth Edition (2010) at Section 1.5.

is a certain type of web browser by sending the header "User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36."

31. TCP (Transmission Control Protocol) is a communication protocol used at the transport layer, which is the layer directly below the application layer in the TCP/IP networking model[10] (or standard Internet protocol stack). TCP is one of the protocols that provide transport of data packets between processes. The TCP protocol is designed to transmit information in packets for logical communication between processes and reliable connection; e.g., the TCP protocol provides information which allows the receiver to re-request packets that were lost (dropped).[11] The TCP protocol encapsulates application data in a packet (or "segment") that includes TCP headers specifying information such as the source and destination ports, sequence numbers, flags, and other data.[12]

32. The networking layer sits below the transport layer in the standard Internet protocol stack and handles the delivery of TCP (or other transport protocol) packets across a network or networks to an intended host (or network "node"). The IP protocol adds an additional header for each packet, which includes required information to route the packet from host-to-host across the network, such as sender and recipient IP addresses. Packets are routed by devices which transfer the packet to its next location based on the information contained in routing tables and rules that attempt to minimize the number of required transfers to send the packet to its recipient. Routing tables can be updated manually or algorithmically, which can change where packets are directed through a given router. Blocking and filtering of network traffic at and around the network layer

[10] https://en.wikipedia.org/wiki/Internet_protocol_suite
[11] https://technet.microsoft.com/en-us/library/bb726993.aspx
[12] See, for example, Kurose J. F. and Ross K. W., "Computer Networking: A Top-Down Approach," Fifth Edition (2010) at Chapter 3.

has been a common practice since at least the 2000s.[13] Furthermore, well-known software such as the Linux "iptables" utility and associated modules have also been readily available since around this time.[14] This software can be used and to perform packet filtering and packet transformation. Functionality such as this can help eliminate contact with known problematic IP addresses or websites, or otherwise assist in managing network traffic.

33. Indeed, the need to restrict communication with known problematic IP addresses, and to otherwise manage network traffic to optimize performance while minimizing risks from network threats, has been well-known at least since the 1990's when the impact of computer viruses, worms, and the like, were widely known in the public domain.[15,16,17] This resulted in a variety of commercially available devices which performed filtering of packets; and such packet filtering was a standard approach to managing network security and optimization well before the priority dates of the patents-in-suit.

34. The link layer resides below the network layer in the standard Internet protocol stack, and this layer is responsible for transmission of data across individual "links" of a network. I.e., it provides the connection between network "nodes." Since this layer resides directly above the physical layer, it can be referred to as "layer two." The link layer further encapsulates network packets with link layer headers and footer information including data such as source and destination MAC addresses. Common link-layer protocols include Ethernet and Wi-Fi.

---

[13] See, for example, Kurose J. F. and Ross K. W., "Computer Networking: A Top-Down Approach," Fifth Edition (2010) at Chapter 8. See also E. Skoudis, T. Liston, "Counter Hack Reloaded: A Step-by-step Guide to Computer Attacks and Effective Defenses" Second Edition (2006).
[14] See, for example, https://netfilter.org/about.html
[15] http://www.cnn.com/TECH/computing/9901/29/iworm-ent.idg/index.html
[16] https://money.cnn.com/2000/05/05/technology/loveyou/
[17] https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

VIII. PRIOR ART BACKGROUND

35. It is my understanding that, as part of the patent application process, an examiner for United States Patent and Trademark Office ("USPTO") undertakes only a limited review of certain prior art.

36. Among other limitations, the examiner does not review any commercially released products, even though such products may be prior art. The examiner's review is limited to other patents and certain published documents, sometimes called nonpatent literature (NPL). Any document used in the rejection of a claim is called a reference.

37. In addition, the examiner does not conduct an exhaustive search of patents or NPL. Instead, the examiner's review is principally based upon: (a) any patents or NPL that the applicant may disclose; and (b) the results of the examiner's first search for patents or NPL. After any first Office action (that is, a document written by an examiner in response to a patent application), the examiner need not ordinarily make a second search of the prior art, unless necessitated by amendments to the claims by the applicant in a reply to the first Office action, except to check to determine whether any reference which would appear to be substantially more pertinent than the prior art cited in the first Office action has become available subsequent to the initial prior art search.

38. The prior art references described in my report were never considered by the USPTO during prosecution of the patents—either because they are commercially-released products and therefore never considered or because they are patents or other NPL that never came to the attention of the USPTO.

IX. THE ACCUSED PRODUCTS

A. NTO 5236 AND NTO 5236 WITH ADVANCED FEATURE MODULE

39. I am informed by counsel that accused products may invalidate a patent if the those same accused products are on-sale before the critical date of the patents and have the same core functionality. I understand that the principle is sometimes expressed as "that which infringes if later, anticipates if earlier."

40. I further understand that Plaintiff has accused the following product models (among others) of infringing each of the patents-in-suit: (1) the NTO 5236 alone; and (2) the NTO 5236 in conjunction with the Net Tool Optimizer Advanced Feature Module (AFM):

> Defendants' Vision ONE Products ("Vision ONE") include the following Vision Series Appliance models: VisionxStream 40, Vision E40, Vision E100, Vision 5236, Vision 5288, Vision ONE, Vision 7300, NTO 5236, NTO 5263, NTO 5268, NTO 5273, NTO 5288, NTO 5293, NTO 7300, and NTO 7303, and Net Tool Optimizer Advanced Feature Module, alone or in conjunction with one another.

Plaintiff's April 20, 2018 Infringement Contentions, Exhs. A-D2.

41. I understand that Defendants have produced evidence showing that: (1) the NTO 5236 and (2) the NTO 5236 in conjunction with the Net Tool Optimizer Advanced Feature Module (AFM) were sold before the critical dates of each of the patents-in-suit.[18] I also understand that Plaintiff does not contest that the products were on-sale before October 22, 2011.

42. The NTO products have the same share similar core functionality. The core functionality of a Net Tool Optimizer is to be a packet broker; that is, to filter packets, aggregate packets, and replicate packets for use by other network tools.[19] For example, each iteration of the NTO 5236 (from the earliest, running with version 2.1.x of the NTO software, to the latest, running with 4.7.x) are intended to perform packet filtering functionality. The earliest as-sold NTO

[18] *See* David Decl. in support of Motion for Summary Judgment; Munson Declaration in support of Motion for Summary Judgment.

[19] I understand that the Ixia has referred to the core functionality of the NTO product line as "NPB [network packet broker] basics" and as "netstack," depending on time. *See* David Depo. at 64:3-20.

5236 directs network data from SPAN ports and TAPs and forwards it to a convenient centrialized tool farm where multiple tools can share simultaneous access to the network data. A core function of the NTO 5236 is depicted here:

1. OVERVIEW

The Anue 5200 Series Net Tool Optimizer directs network data from SPAN ports and TAPs in your data center and forwards it to a convenient centralized tool farm where multiple tools can share simultaneous access to the network data.

The Anue 5200 has a full range of connectivity capabilities so each network tool is fed exactly the data it needs from anywhere in your network.

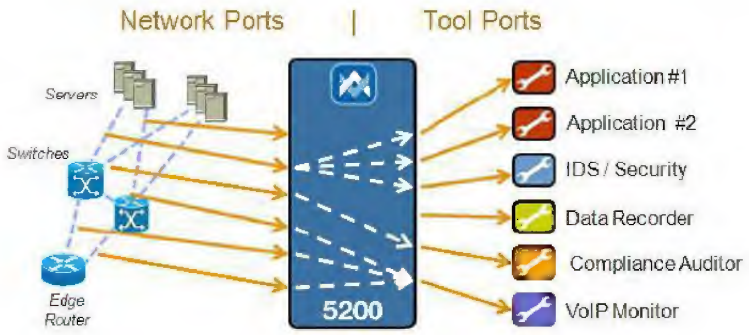


Figure 1 - Anue 5200 Tool Optimization

Inbound traffic from any incoming port may be switched to one or more outgoing ports, regardless of the speed of the incoming and outgoing ports. Note that traffic flows through the Anue 5200 unidirectionally from a network port through a filter to a tool port.

5200 Series Manual at 5.

43. The NTO 5236 can be used to filter packets based on several different filter-criteria options, including as follows:

Filter Criteria Options

The following filter criteria are available to define the type of traffic that will pass through a filter. Note that Filters (filter objects display in the center of the diagram area) and Tool Ports both have filter criteria settings. **Filters allow traffic** to pass through them based on the defined criteria; **Tool Ports deny traffic** from passing through them based on the defined criteria.

The following filter criteria options are available:

- MAC Address (not available for tool ports)
- VLAN Tag
- Ethertype (not available for tool ports)
- IPv4 Address
- IP Protocol
- DSCP/TOS
- TCP/UDP Port
- TCP Control (for 5236 only)

Several criteria options can be selected per filter. The selected criteria can be "anded" "or'd". A filter can also be configured to Pass All traffic or Drop All traffic.

5200 Series Manual at 8.

44. The NTO 5236 can be used to aggregate data traffic, as illustrated in "Use Case 1" for the NTO 5236 product:

Use Case 1: Aggregating 3 Network Ports to One Tool Port

A common use for the Net Tool Optimizer is to aggregate traffic from many network ports to one tool port. The aggregation can give a tool a "big pipe view" and alleviate the need to use multiple tools.

The diagram below shows how three network ports have been aggregated to one tool port by drawing connectors from the network port to a filter and then from the filter to the tool port.

Step-by-step instructions on how to create a configuration like the one shown in the figure below can be found in the Quick Start Example.



Figure 101 - Three Networks Ports Aggregated to One Tool Port

5200 Series Manual at 86.

45. The figure above shows that three 1 Gig ports have been aggregated to one 1 Gig port. The applied filter (VLAN 10) eliminates traffic that is not required by the Data Capture tool port at the far right-hand side of the diagram and prevents the three network ports on the left-hand side from causing a packet overflow at the tool port.

46. The NTO 5236 can be used to replicate data traffic for use by more than one network tool, as illustrated in "Use Case 3" for the NTO product:

Use Case 3: Sending SPAN Port Data to Several Devices

A common problem that occurs with a SPAN port is that there often contention for the data on the SPAN port as other network priorities arise. This problem is easily resolved when the SPAN port is connected to the Anue 5200. A second tool port is simply added and connected to the filter and the 2nd device is physically connected to the Anue 5200.

In the figure below notice that Filter 1 is passing all traffic from Router SPAN Port 3 (P04) to the IPS (P22) tool port.

The tool port icon indicates that a layer 4 Source Port deny criterion has been configured (L4SPT). The tool port is configured to deny DNS source port (53) traffic.



Figure 110 - SPAN Port Data Sent to One Tool

Create the second tool port for a traffic analyzer and draw a connector to the Pass All Filter. The second tool port is configured to **Pass All** traffic.

In the figure below the Router SPAN Port 3 traffic is now being sent to two tool ports. The IPS (P22) tool port is denying or filtering a portion of the available traffic, the Traffic Analyzer (P20) tool port is receiving all of the available traffic.



Figure 111 - SPAN Port Data Sent to Two Tools

5200 Series Manual at 92-93.

CENTRIPETAL-CSCO 087526

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 26

47. Through the application of the "pass all filter," the NTO 5236 is sending all network traffic originating from the Router SPAN port to two different destination tool ports—the Intrusion Prevention System and the Traffic Analyzer.

48. The NTO 5236 with Advanced Feature Module[20] can be used to filter packets, aggregate packets, and replicate packets for use by other network tools, as set forth above. The Advanced Feature Module[21] added a set of packet processing features to supplement the core filtering, aggregation, and replication being done by the NTO 5236. Those features are as follows:

    a. Packet De-Duplication - Eliminates redundant data packets generated from the TAPs and SPAN ports at full line rate to monitoring tools, significantly improving tool bandwidth.

    b. Packet Trimming - Trims packet payload before the packet arrives at the monitoring or security tool to improve tool bandwidth

    c. Multi-Protocol Label Switching ("MPLS") Stripping - Enables non-MPLS capable monitoring tools to monitor MPLS data by removing MPLS labels from the packet stream and leaving the inner (tunneled) packets header exposed.

    d. Extended Burst Protection - Prevents dropped packets when aggregating multiple network streams into a single 1 Gig stream ensuring monitoring tools always receive the data they need.

KEYSIGHT_0013123;
https://www.ixiacom.com/products/vision-5236-nto-5236
(Description of packetstack)

---

[20] I understand that the Ixia has referred to the features in its Advanced Feature Module as "AFM" or as "packetstack," depending on time. *See* David Depo. at 93:17-100:6.
[21] See, PA0000768, PA0000840 and PA0001127—1154.

X. U.S. PATENT NO. 9,137,205

49. I have been asked to review the '205 patent and assess the validity of Claims 17 and 33. First, I will summarize the '205 patent briefly and then discuss a claim-by-claim invalidity analysis.

B. SUMMARY OF THE '205 PATENT

50. The '205 patent assigned to Centripetal Networks, Inc., Herndon, VA (US), was filed on Oct. 22, 2012 and published on Sept. 15, 2015. The '205 patent relates to methods and systems for protection of secured networks. Specifically, it relates to packet filtering of network traffic using security policy management (SPM) servers and packet security gateways (PSGs). Figure 1 illustrates an exemplary network environment protected using the methods and systems disclosed in '205 patent. In this example, there are four PSGs located at the borders of four LANs (local area networks). These PSGs can protect their respective networks from the incoming packets sent via Network E in the example (e.g. the Internet). This example also includes one SPM server that communicates dynamic security policies to PSGs.[22]

[22] '205 Patent at 4:12 – 5:23.

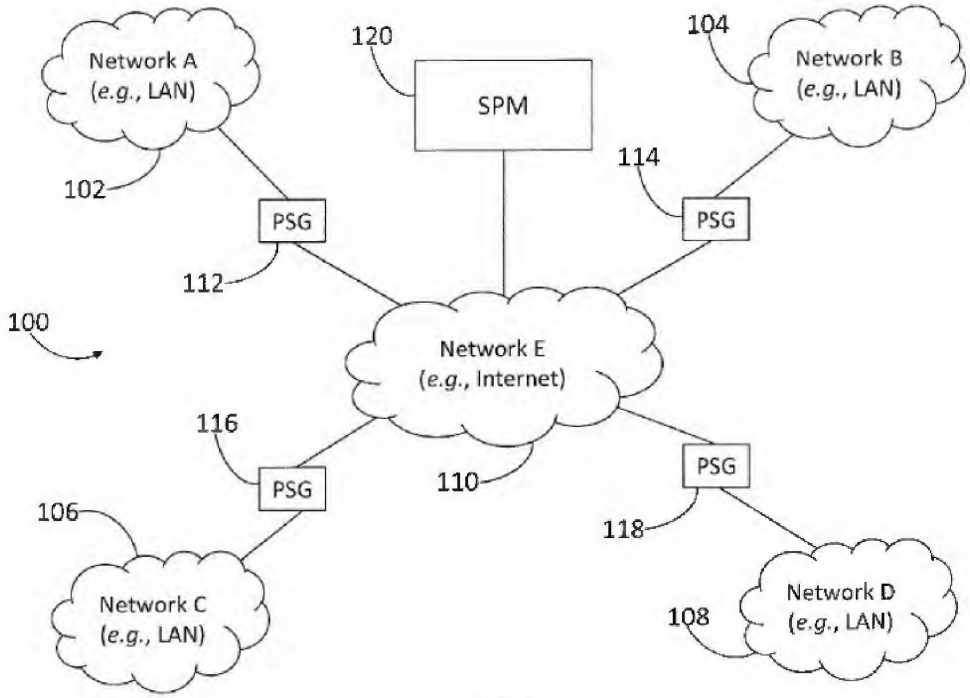


FIG. 1

Figure 1. An exemplary network environment protected by methods and systems disclosed in the '205 patent ('205 Patent, FIG. 1).

51. A security policy management server is a computing device that is configured to communicate a dynamic security policy to a packet security gateway.[23] Figure 2 illustrates an exemplary SPM including memory, processor, management interface, and network interface (NI). The memory in SPM stores various program modules and dynamic security policies, which include criteria corresponding to one or more packets and a packet transformation function to be performed on packets corresponding to the specified criteria.[24] The processor executes program modules to configure SPM to (1) communicate dynamic security policies to PSGs, (2) receive updates from malicious host tracker services, and (3) automatically alter or create one or more rules related to malicious network traffic. The management interface provides administrators

[23] '205 Patent, at 4:37-40.
[24] '205 patent, at 4: 44-47.

access to SPM via a graphical user interface (GUI) or a command line interface (CLI). Administrators can use management interface to add PSGs and to construct new dynamic security policies.

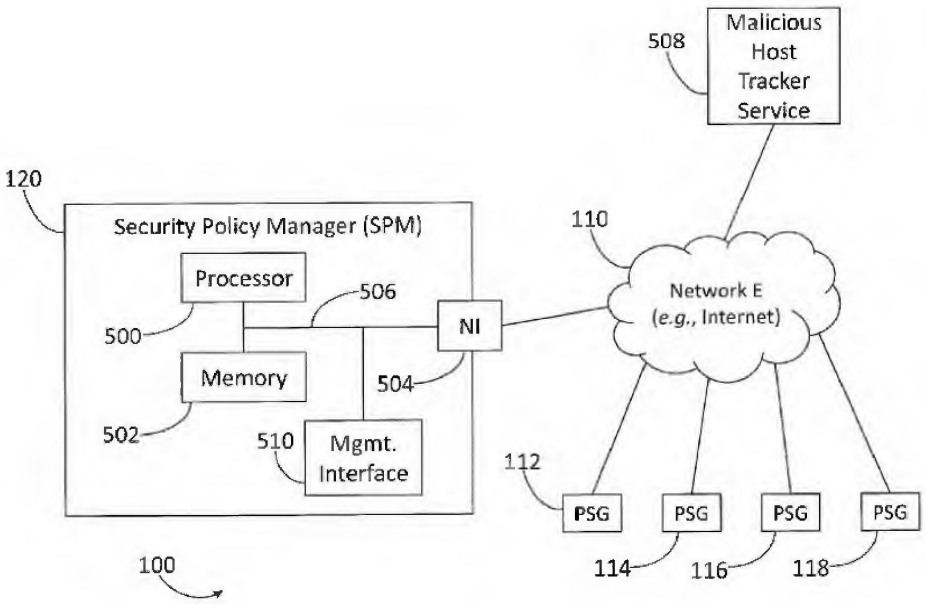


FIG. 5

Figure 2. An exemplary security policy manager (SPM) disclosed in the '205 patent ('205 Patent, FIG. 5).

52. A packet security gateway is a computing device configured to receive and filter packets and perform a packet transformation on the packets.[25] Figure 3 illustrates an exemplary SPG including the following components: processor, memory, NIs, management interface and packet filter. The processor configures the SPG by executing one or more program modules included in the memory. The PSG receives dynamic security policies from the SPM via the management interface or the network interface. Packet filters examine incoming packets in comparison with dynamic security policies and information associated with the packets received by PSG. Based

[25] '205 Patent, at 4:33-35.

on the results of this analysis, the packet filters can apply one or more packet transformation functions (PTF), e.g., forward, drop, or other functions.

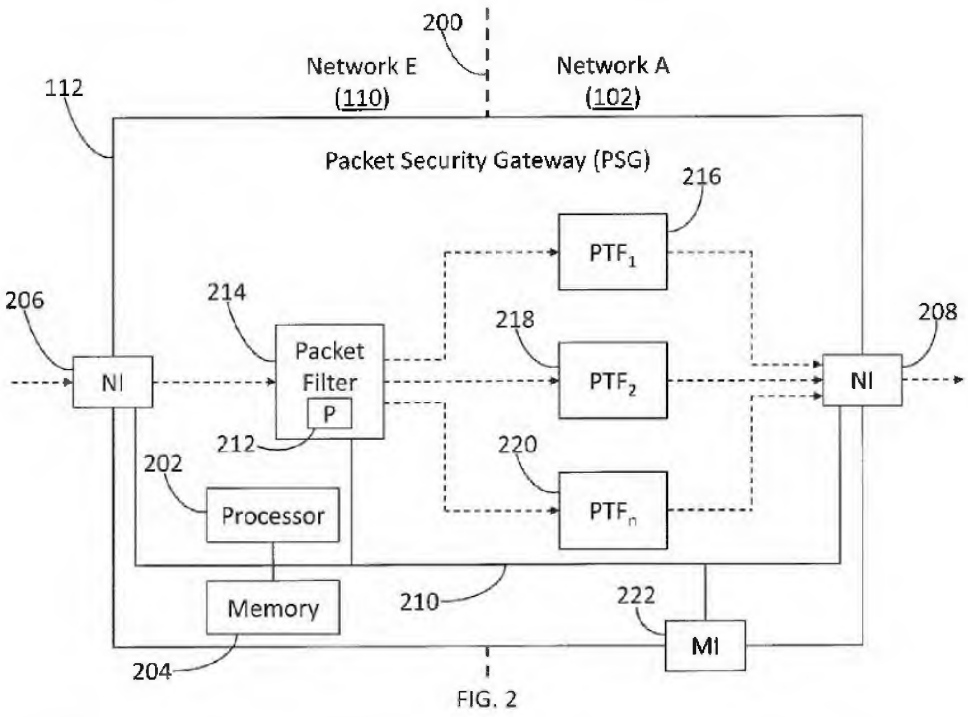


Figure 3. An exemplary packet security gateway (PSG disclosed in the '205 patent. ***'205 Patent, FIG. 2.***

C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF TIPPINGPOINT IPS

53. The TippingPoint UnityOne-200 Intrusion Prevention System ("TippingPoint IPS" or "TippingPoint system") is a network security solution to protect virtual and physical networks, applications, and data against a range of network security threats. This system performs the functions of two packet security gateways and one security policy management server, and a typical usage case for the system is to identify packets that correspond to criteria so that a criteria-specific action (e.g. blocking, logging, forwarding, re-routing, or the like) may be applied on a packet-by-packet basis to network traffic.

54. The TippingPoint system was commercially available to purchase prior to the priory date of the '205 Patent. For example, the startup log for the TippingPoint device Exponent procured for testing (see below) shown in Figure 4 below indicates that the build date for this system was January 25, 2008.



Figure 4: Excerpt from startup sequence log for the TippingPoint Unity One 200 device tested by Exponent.

55. Other material also shows that the TippingPoint system was commercially available to purchase prior to the priory date of the '205 Patent. Examples include as follows:

    a. On June 16, 2003, TippingPoint announced the availability of UnityOne-200 in a press release, mentioning the Digital Vaccine service as part of "[e]ach of the UnityOne Intrusion Prevention Systems and Appliances." (https://web.archive.org/web/20030821160654/http://www.tippingpoint.com:80/news_events/pdf/UnityOne200_061603.pdf).

    b. On June 18, 2003 Enterprise Systems Journal published an article discussing "TippingPoint's just-released UnityOne 200 appliance" and mentioning the "digital vaccines" that are UnityOne filters. June 18 2003 Enterprise Systems Journal Article, Protecting Data From Events Firewalls Can't Catch -- Enterprise

Systems (https://esj.com/articles/2003/06/18/protecting-data-from-events-firewalls-cant-catch.aspx).

c. On October 3, 2003 WayBack Machine captures of the TippingPoint website, a UnityOne product brochure and Peer-to-Peer Piracy Prevention datasheet list the UnityOne-200 product as one of TippingPoint's platforms. (https://web.archive.org/web/20031003183758/http://tippingpoint.com:80/resource_library/pdfs/TPTI_Quickie.pdf); (https://web.archive.org/web/20031003204905/http://tippingpoint.com:80/resource_library/pdfs/PPPP_Data_Sheet.pdf).

d. On a December 7, 2003 WayBack Machine capture of the TippingPoint website, a UnityOne DataSheet includes UnityOne-200 in a list of systems. (https://web.archive.org/web/20031207030351/http://www.tippingpoint.com:80/resource_library/pdfs/200-400-1200-2400_DataSheet.pdf).

56. For at least the reasons detailed below, it is my opinion that the TippingPoint system enabled a person of ordinary skill in the art to practice each and every element of Claims 17 and 33 of the '205 Patent, and that a POSITA would be motivated to do so as part of the typical routine of setting up standard network protection mechanisms. Thus, it is also my opinion that the TippingPoint IPS anticipates these claims. In addition to the analysis presented herein, further discussion of relevant testing is described in Appendix B, which I incorporate by reference.

1. TEST CONFIGURATION WITH TIPPINGPOINT IPS

57. Exponent procured a TippingPoint IPS device with part number SBASY-199 Rev: C03 and serial number ST05170004, as shown in Figure 5.



Figure 5. TippingPoint IPS hardware showing the part number and serial number of the device.

58. The TippingPoint system includes a local security manager (LSM) program, which "is the control center from which you can configure, monitor, and report on the UnityOne Intrusion Prevention System (IPS) devices in your network."[26] The TippingPoint IPS also includes two separate Ethernet port pairs called "segments"; each segment can be programmed to follow its own set of filtering rules via the LSM.

59. The TippingPoint IPS LSM includes "a graphical user interface (GUI) that enables you to monitor and configure your UnityOne Intrusion Prevention System (IPS) using an ordinary web browser."[27] For Exponent's testing, a computer running Windows XP was connected via Ethernet cable to the MGMT Ethernet port of the TippingPoint IPS, which is indicated with

[26] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. xi.
[27] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 8.

red annotations in Figure 6, and Internet Explorer 7 was used to access the TippingPoint IPS GUI from this computer.[28]



Figure 6. Annotated photographs of the TippingPoint IPS showing two packet security gateway interfaces (lower left) and one management interface (lower right).

60. The physical configuration of the test setup used for Exponent's analysis is shown in Figure 7. This figure shows the physical layout of the hardware, including the IPS with its two segments (SEG 1 and SEG 2), the computer used to connect to the LSM interface (labeled "LSM"), two switches, and three additional laptop computers (Computers A, B, and C) for sending and receiving packet traffic.

[28] The TippingPoint IPS web server was found to be incompatible with modern versions of Internet Explorer. Internet Explorer 7 was released circa 2006. (See, for example, https://en.wikipedia.org/wiki/Internet_Explorer_version_history#Windows_Internet_Explorer_7.)

CENTRIPETAL-CSCO 087535

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 35

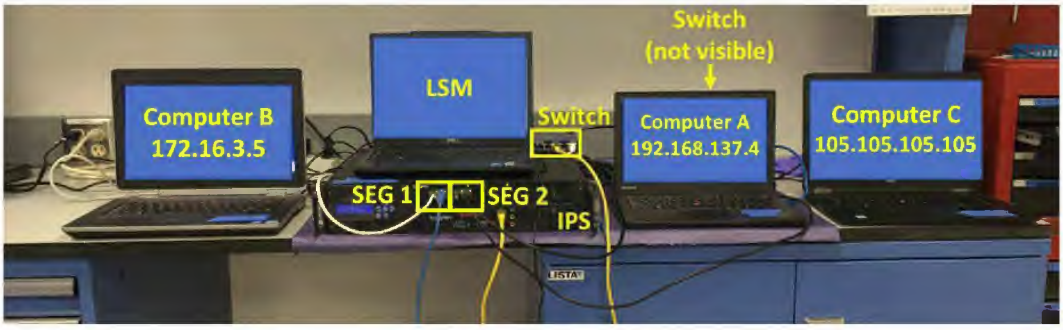


Figure 7. Image of test network used as part of the claim analysis that shows a hardware installation of one IPS containing a local security management (LSM) interface. The laptop labeled LSM is used to connect to the LSM. Computers A, B, and C reside in separate network address spaces and are connected by the two segments.

61. The test configuration shown in Figure 7 includes computers with IP addresses in three different network address spaces. Only two of these computers (and only one TippingPoint IPS segment) are required to demonstrate how the TippingPoint system satisfies the requirements of Claims 17 and 33.[29]

62. A first network, called "Network A," includes IP addresses in the range from 192.168.1.37.2 through 192.168.137.5, which contains Computer A. Network traffic internal to Network A is communicated via a TP-Link TL-SG108 Switch (not visible in Figure 7). A second network, called "Network B," includes a computer with IP address 172.16.3.5, which is Computer B.

63. Network A and Network B are used to illustrate how the TippingPoint system satisfies the requirements of Claims 17 and 33. Network A and Network B are connected by the first segment, which is the segment labeled SEG 1 in Figure 7.

64. The test network shown in Figure 3 also includes a third network, called "Network C," that includes a computer with IP address 105.105.105.105, labelled "Computer C." Network A

[29] Prior to Plaintiffs' Centripetal Networks, Inc.'s Identification of Asserted Claims, dated June 22nd, 2018, claims 91, 93, and 95 were also at issue in this litigation; these claims required a third network, and Network C was used for demonstrating that these claims were also satisfied by the TippingPoint system.

and Network C are connected by the second segment, which is the segment labeled SEG 2 in Figure 3.

65. Figure 8 shows the schematic layout of the networks described above. Network A includes Computer A, as well as other IP addresses as indicated in the figure; Network B includes Computer B; and Network C includes Computer C. The first TippingPoint system segment (SEG 1) protects Network B from Network A; and the second segment (SEG 2) protects Network C from Network A.

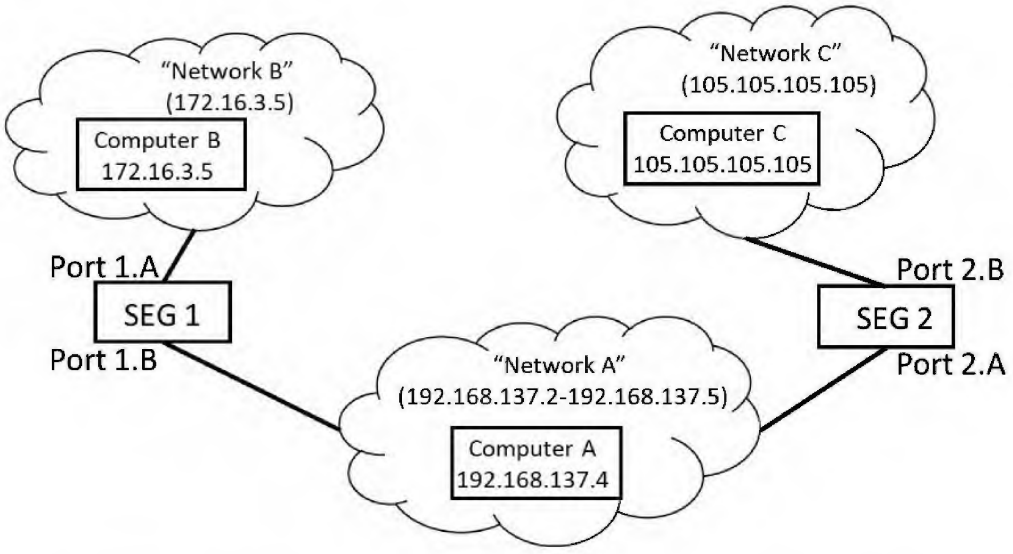


Figure 8. Schematic of the test network (see Figure 7) architecture, including the static IP addresses of each element. Each network has its own subnet. SEG 1 protects Network B from Network A. SEG 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (Port A and Port B), which are used to pass traffic between networks

66. As detailed below, this test configuration enables demonstration of Claims 17 and 33 of the '205 Patent.

2. CLAIM 17

67. **Claim 17a: A system, comprising: security policy management server; and one or more packet security gateways associated with the security policy management server,**

CENTRIPETAL-CSCO 087537

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 37

wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to. As detailed below, the TippingPoint system satisfies all requirements of this claim element.

68. The '205 Patent states that "[a]s used herein, a security policy management server includes any computing device configured to communicate a dynamic security policy to a packet security gateway."[30] I understand, however, that the parties have agreed that the term "security policy management server" is to be construed as "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway,"[31] and I have applied this claim construction throughout my analysis. The TippingPoint system comprises a security policy management server, for at least the following reasons.

69. The TippingPoint system includes a local security manager (LSM) program, which "is the control center from which you can configure, monitor, and report on the UnityOne Intrusion Prevention System (IPS) devices in your network."[32] As detailed in relation to Figure 6, the LMS program is accessed via a web server running on the MGMT Ethernet interface of the TippingPoint IPS. As detailed below in relation to other claim elements, this server enables access to a graphical user interface (GUI) with which dynamic security policies may be managed and communicated to the TippingPoint security gateways. Therefore, the TippingPoint includes "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway," as required by the claim construction of "security policy management server." Also, although I have applied the agreed upon claim constructions throughout my analysis, the TippingPoint system also satisfies the definition

[30] '205 Patent, at 4:37-40.
[31] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.
[32] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. xi.

CENTRIPETAL-CSCO 087538

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 38

for "security policy management server" stated within the '205 Patent, at least because the laptop running the TippingPoint LSM constitutes a "computing device configured to communicate a dynamic security policy to a packet security gateway," which is broader than the agreed upon construction.

70. The '205 Patent states that "[a]s used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation on the packets."[33] I understand, however, that the parties have agreed that the term "packet security gateway" is to be construed as "a gateway computer configured to receive packets and perform a packet transformation function on the packets,"[34] and I have applied this claim construction throughout my analysis.

71. I also understand that there is a dispute regarding the construction of the term "packet transformation function." More specifically, Plaintiffs have proposed that this term be construed as "function that transforms packets from one state to another" while Defendants have proposed "an operation performed on a packet specified by the dynamic security policy, such as forward or drop."[35] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system comprises "one or more packet security gateways," as detailed below.

72. The TippingPoint system includes two separate Ethernet port pairs called "segments," which are labeled "SEG 1" and "SEG 2" in Figure 6, that act as two separate packet security gateways where each security gateway can be programmed independently to follow its own set of filtering rules via the LSM. For example, as discussed in relation to Figure 6 and

[33] '205 Patent, at 4:33-35.
[34] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.
[35] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

CENTRIPETAL-CSCO 087539

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 39

Figure 7, each security gateway segment receives packets traveling between networks, and then applies filtering rules to these packets. More specifically, in Exponent's test setup described above, segment 1 is located at the boundary between Network A and Network B, and receives all packets that pass between these two networks. Upon receiving packets, a computer within the TippingPoint IPS applies rules according to the currently applied security policy. Thus, the TippingPoint system includes "a gateway computer configured to receive packets" as required by the agreed upon construction for "packet security gateway."

73. As discussed above, there is a dispute as to the interpretation of "packet transformation function." However, the TippingPoint system satisfies both parties' proposed construction for this term for at least the reasons herein. Plaintiff's proposed construction of "packet transformation function" requires a function that "transforms one or more packets from one state to another." Although Plaintiff's have not provided an explicit definition for transforming "from one state to another," the intrinsic evidence cited to by Plaintiff in support of their proposed construction includes example embodiments in which packets are forwarded or dropped depending upon parameters of the packet such as the origination IP address. Thus, under Plaintiff's proposed construction, forwarding or dropping of packets constitutes transforming a packet from one state to another, and hence forwarding or dropping satisfy Plaintiff's construction of "packet transformation function." Similarly, Defendants' proposed construction for "packet transformation function" explicitly includes the operations "forward or drop," and hence forwarding or dropping also satisfy Defendant's proposed construction for this term. As detailed below in relation to other claim elements, the TippingPoint IPS can perform a variety of functions upon the received packets, depending upon the rules within the current policy and parameters of the received packets, including but

not limited to: forwarding packets to their intended address; forwarding packets to an address other than their intended address; dropping packets; logging or otherwise monitoring packets. Therefore, the TippingPoint IPS satisfies both parties' proposed construction for "packet transformation function."

74. Therefore, for at least the reasons above, each of the TippingPoint IPS segments constitutes "a gateway computer configured to receive packets and perform a packet transformation function on the packets," and hence the TippingPoint system comprises "one or more packet security gateways," as required by this claim element as construed by both parties.

75. Furthermore, the TippingPoint security gateway segments are each "associated with the security policy management server" at least because the security policies, and associated rules, applied by each segment are configurable using the LSM program via the webserver running on the MGMT Ethernet interface. Also, each of the TippingPoint security gateway segments "comprises computer hardware and logic," as required by this claim element; and, as detailed below in relation to the subsequent elements of claim 17, said computer hardware and logic is "configured to cause the packet security gateway [segments] to" satisfy all requirements of claim 17 of the '205 Patent.

76. Consequently, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17a of the '205 Patent.

77. **Claim 17b: receive a plurality of dynamic security policies from the security policy management server.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

78. I understand there is a dispute regarding the construction of the term "dynamic security policy." More specifically, Plaintiff has proposed that this term be construed as "a non-static

set of one or more rules, messages, instructions, files, or data structures associated with one or more packets," while Defendants have proposed that this term be construed as "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria".[36] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of this claim element, for at least the reasons detailed below.

79. For at least the reasons set forth in relation to claim element 17a, the TippingPoint's LSM and associated web server comprise a "security policy management server," as required by this claim element and the associated claim construction agreed upon by both parties; and, the TippingPoint's security gateway segments each constitute a "packet security gateway," as required by this claim element and the associated claim constructions.

80. Using the test setup described above, Exponent has demonstrated that the TippingPoint security gateway segments receive dynamic security policies from the LSM and associated web server. The TippingPoint system includes 1,888 filters that are available by default on the TippingPoint IPS, fifteen of which are shown in Figure 9. Each of these filters comprise at least one rule that can be adjusted to perform various user-defined packet transformation functions upon packets associated with said rule, e.g. forwarding, dropping, logging, copying, etc., on packets that correspond to relevant criteria: i.e. each filter, which constitutes at least one rule, contains at least one criteria, and at least one packet transformation function that is to be applied to packets that are associated with the filter by satisfying the criteria.

[36] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

Thus, each filter comprises at least one rule that satisfies both the proposed constructions for "dynamic security policy."

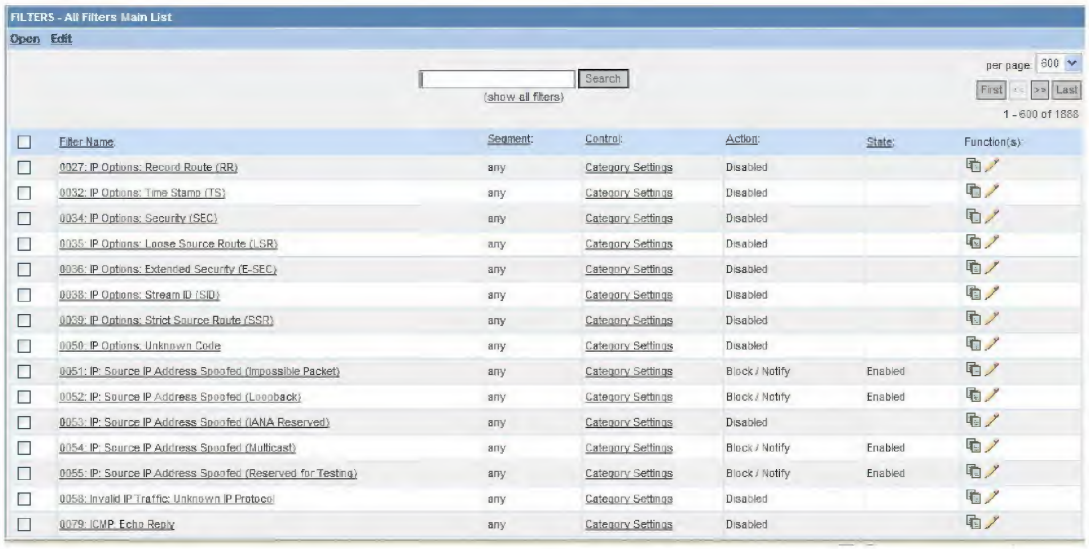


Figure 9. Sample filters available in the IPS.

81. For example, Figure 10 below shows a screen shot from the settings window, accessed via the LSM GUI, for a filter called "0361:HTTP:Protected File Access (/etc/passwd)." This filter detects HTTP requests that are attempting to access the password file on a Unix system, which is typically stored in file /etc/passwd: i.e. the criteria for this filter is satisfied by any packets that are attempting to send a request to access /etc/passwd. The dropdown menu that is also shown in this figure contains a list of "actions" that can be selected: these actions define the packet transformation function that will be performed upon packets that match the criteria of the filter.

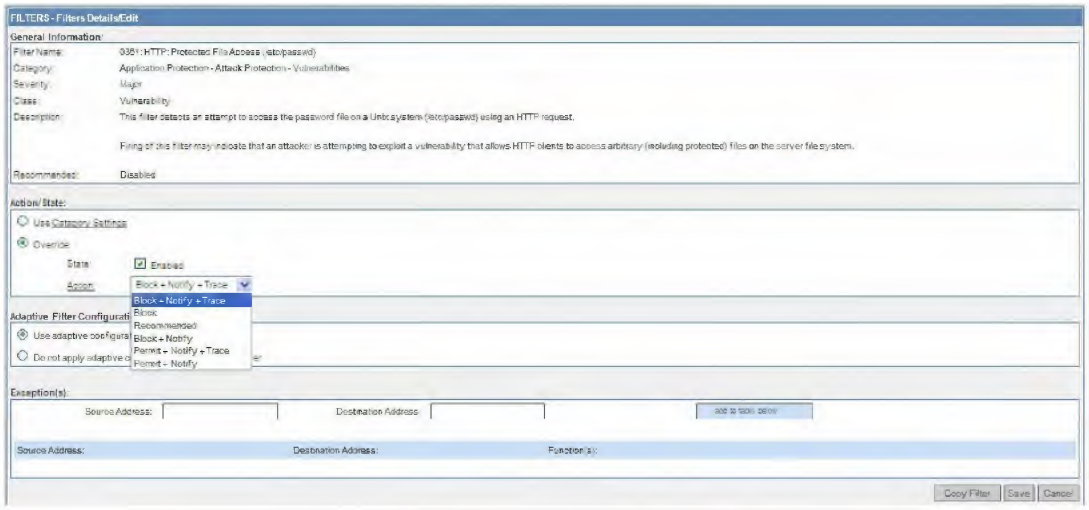


Figure 10. Filter 0361, which "detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request." A series of actions are possible for packets that are identified by this filter.

82. Exponent's testing confirms that the available "actions" correspond to packet transformation functions. For example, if the action is set to "Block" then packets that match the filter criteria are prevented from reaching their intended destination (i.e. are dropped) and also logged in a Block Log. Figure 11 below shows the Block Log after a single packet that matches the 0361:HTTP:Protected File Access (/etc/passwd) filter criteria has been sent between Networks A and B while the "action" was set to "Block." As another example, if the action is set to "Permit" then packets that match the filter criteria are allowed to pass to their intended destination (i.e. are forwarded), but are also logged in an Alert Log. Figure 12 shows the Alter Log after a single packet that matches the 0361:HTTP:Protected File Access (/etc/passwd) criteria has been sent between Networks A and B while the "action" was set to "Permit + Notify." Thus, the 0361:HTTP:Protected File Access (/etc/passwd) filter implements a rule that is associated with packets that attempt to access the /etc/passwd file, and can perform at least the "forward" or "drop" packet transformation functions upon packets that satisfy this criteria. Therefore, this example filter has been demonstrated to

constitute a "dynamic security policy" that is received by the TippingPoint security gate segment 1 from the TippingPoint LMS and associated web server.

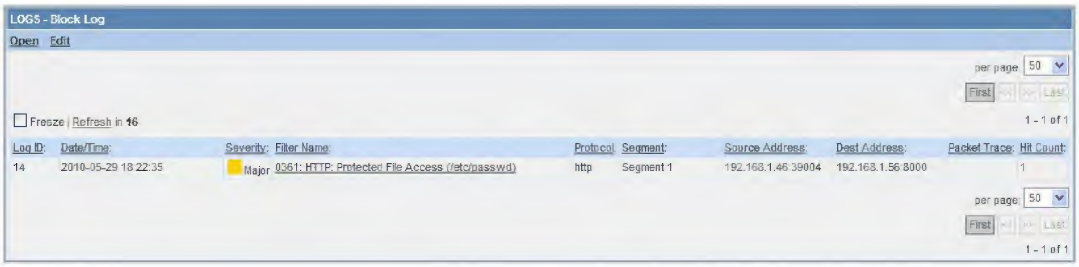


Figure 11. Block Log, which shows the blocked packets.



Figure 12. Alert Log that shows packets that the filter identified but allowed to pass through the gateway.

83. Furthermore, the TippingPoint dynamic security policies may be comprised of more than one filter, that each may have its own criteria and corresponding packet transformation function. For example, Figure 13 shows a sample of the TippingPoint traffic management filters screen with eight filters entered: this set of traffic management filters also comprises a "dynamic security policy" that satisfies both proposed constructions for this term.

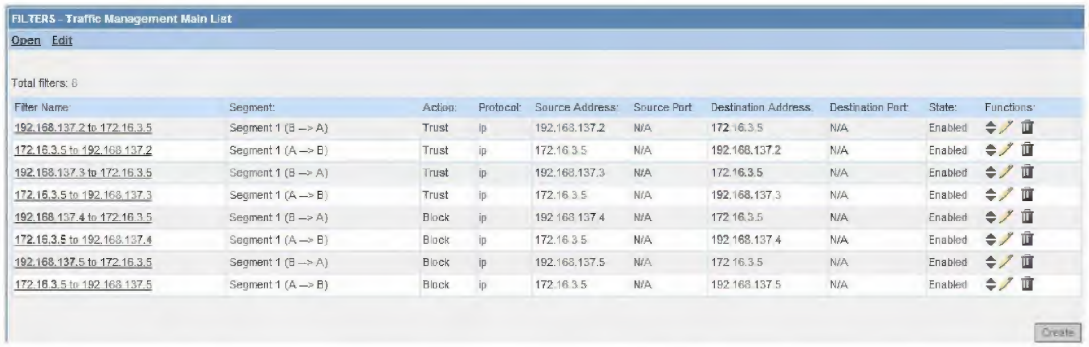


Figure 13. Traffic management filters

84. Each traffic management filter can be customized through various parameters, and in general is configured to perform one of the available "actions" upon packets that are being sent between specified origination and destination IP addresses; i.e. the criteria for the traffic management filters are based upon the source and destination IP addresses of the packets. A screenshot displaying the parameters that can be used to customize a traffic management filter is shown in Figure 14; from this window, the "source" and "destination" IP addresses for the filter's criteria may be altered, as well as the action to be performed upon packets that satisfy these criteria. The "save" button in the lower right corner creates/updates the filter with the customized settings.

CENTRIPETAL-CSCO 087546

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 46

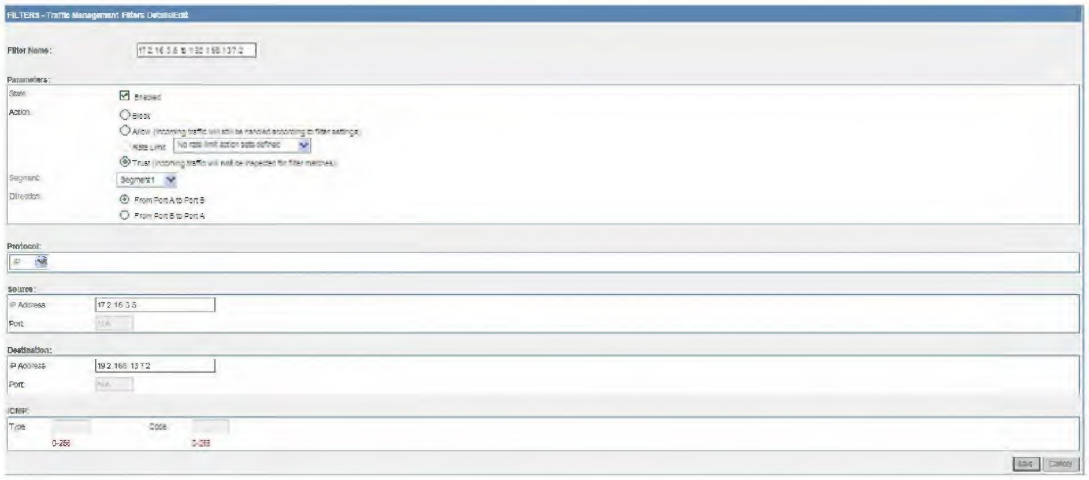


Figure 14. Parameters for defining a traffic management filter. The "save" button in the lower right corner creates the filter.

85. The TippingPoint system may receive a plurality of dynamic security policies. For example, the "Allow" setting within the traffic management filters (which themselves constitute a dynamic security policy as explained above) shown in Figure 14 causes packets that match the filter criteria to be inspected against the other dynamic security policies within the system, while the "Trust" setting causes said packets to be forwarded without being inspected against other dynamic security policies.[37] In addition, the TippingPoint system can receive a plurality of dynamic security policies sent in sequence at different times from the TippingPoint LSM and associated web server, as is explained below in relation to subsequent elements of claim 17.

86. Thus, as explained above, the TippingPoint security gateway segments receive a plurality of dynamic security policies from the TippingPoint LSM and associated web server, and this satisfies all requirements of claim element 17b of the '205 Patent.

---

37 "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 89.

87. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17b of the '205 Patent.

88. **Claim 17c: receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

89. I understand there is a dispute regarding the construction of the term "rule." More specifically, Plaintiff has proposed that this term be construed as "condition or set of conditions that when satisfied cause a specific action to occur," while Defendants have proposed that this term be construed as "(i) packet-identifying criteria and (ii) a function to be performed on the identified packets."[38] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of this claim element, for at least the reasons detailed below.

90. As discussed in relation to claim element 17b, the TippingPoint system is able to implement rules that specify a set of network addresses for which packets should either be forwarded or dropped. These rules satisfy both the proposed claim constructions. For example, these rules contain a "condition or set of conditions" based upon the IP addresses associated with received packets, and cause "a specific action to occur" (e.g. forward or drop) when packets satisfy said condition or set of conditions. Thus, Plaintiff's proposed construction is satisfied. Also, for these rules the associated IP addresses of received packets are used as a "packet-

[38] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

identifying criteria" and "a function" (e.g. forward or drop) is "performed on the identified packets": thus, Defendants' proposed construction is also satisfied.

91. That the TippingPoint system satisfies all requirements of this claim element has been demonstrated using the test setup discussed above in relation to Figure 7 and Figure 8, as described herein. Using the TippingPoint LSM an initial dynamic security policy containing eight explicit rules was created, a screenshot from the LSM GUI showing these rules is shown in Figure 15. This dynamic security policy was communicated to the TippingPoint IPS security gateway segments via the associated web server.

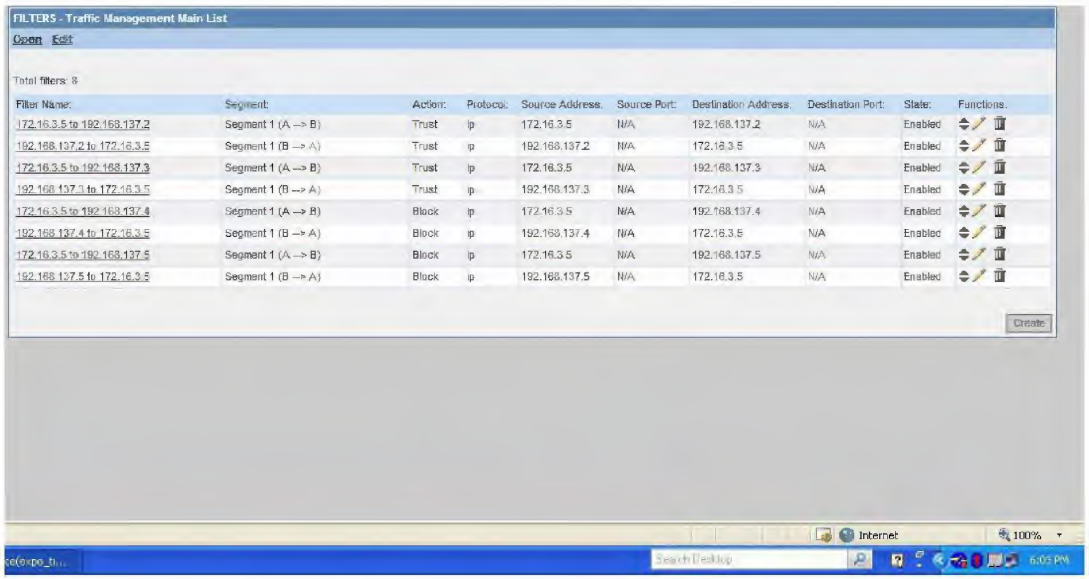


Figure 15. Screenshot of The LSM GUI showing the first dynamic security policy with eight explicit rules. The top four rules allow packet transmission, and the bottom four rules block packet transmission.

92. The eight explicit rules specify whether packets are forwarded or blocked depending upon the IP addresses associated with said packets. More specifically, the first two rules cause any packets between IP addresses 192.168.137.2 and 172.16.3.5 to be forwarded; and the second two rules cause any packets between IP addresses 192.168.137.3 and 172.16.3.5 to be

forwarded. Thus, the first four rules constitute "at least one rule specifying a set of network addresses for which associated packets should be forwarded," as required by this claim element. Furthermore, rules 5 – 8 are configured to cause network traffic outside of this set of network addresses for which associated packets should be forwarded to be dropped. More specifically, rules 5 and 6 cause all packets between IP addresses 192.168.137.4 and 172.16.3.5 to be dropped; and rules 7 and 8 cause all packets between IP addresses 192.168.137.5 and 172.16.3.5 to be dropped. Thus, rules 5 to 8 constitute rules specifying "network addresses outside of the set of network addresses for which packets should be forwarded," and these rules also specify that all packets that match the rules' criteria should be dropped. Therefore, communication of the above example dynamic security policy satisfies all requirements of claim element 17c.

93. To demonstrate the above dynamic security policy shown in Figure 15, said policy was installed on the TippingPoint security gateway segment 1, and ping attempts were made between Computer A and Computer B. Computer A is within Network A, and has IP address 192.168.137.4; Computer B is within Network B, and has IP address 172.16.3.5. Thus, according to rules 5 and 6, all packets between these computers should be dropped by TippingPoint security gateway segment 1. A ping attempt was made from Computer B to Computer A, and from Computer A to computer B, as shown below in Figure 16 and Figure 17 respectively; note that by default a command line "ping" function makes four ping requests, and, as is seen below in screenshots from Computer A and Computer B, all ping requests timed out because the TippingPoint security gateway segment dropped the associated packets.

CENTRIPETAL-CSCO 087550

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 50

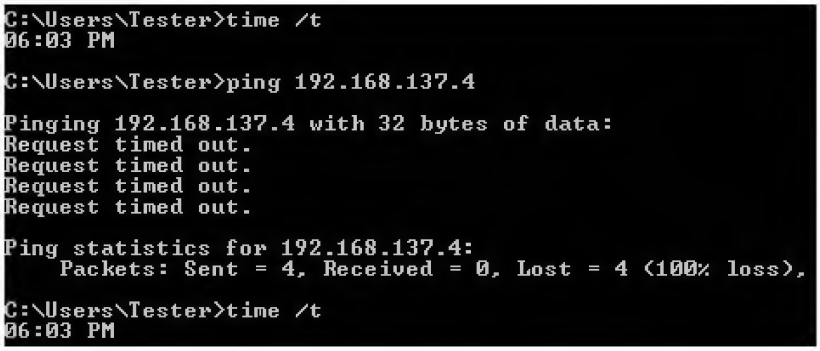


Figure 16. Attempt to ping Computer A from Computer B.

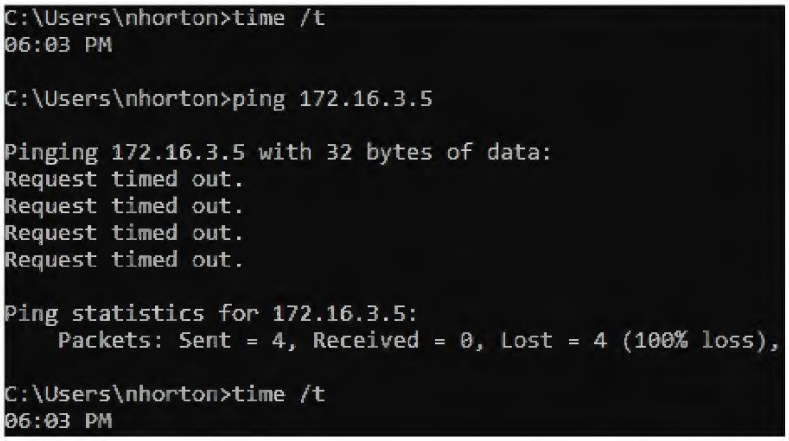
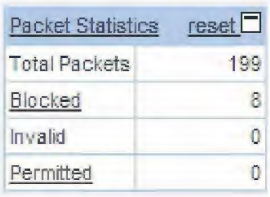


Figure 17. Attempt to ping Computer B from Computer A

94. That the ping request packets were received by the TippingPoint security gate and dropped is further supported by the "Packet Statistics" panel within the TippingPoint LSM GUI. The packet statistics were reset prior to the above-described ping requests, however, after the four ping requests were sent from each computer, 8 "Blocked" packets were reported as shown in the screenshot below in Figure 18.



Packet Statistics	reset
Total Packets	199
Blocked	8
Invalid	0
Permitted	0

Figure 18. The eight blocked packets comprise the four ping requests from Computer A to Computer B, and the four ping requests from Computer B to Computer A

95. Thus, the ping requests above have demonstrated behavior consistent with the dynamic security policy outlined in relation to Figure 15, which, as explained above, satisfies all elements of claim element 17c.

96. In addition, in the event that claim element 17c is interpreted to require that *all network addresses* outside a set of network addresses for which packets should be forwarded to be dropped, as opposed to dropping *all packets* associated with network addresses outside of said set, the TippingPoint system still satisfies all requirements of this claim element. Although rules 5 to 8 in the above example specify an explicit range of IP addresses (which are outside of the set of network addresses for which packets should be forwarded as per rules 1 to 4), a POSITA would recognize that more rules could have been configured to block packets between *all* network addresses outside of the range forward per rules 1 to 4.

97. Thus, for at least the reasons above, it is my opinion that the TippingPoint system satisfies all requirements of element 17c of the '205 Patent.

98. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17c of the '205 Patent.

99. **Claim 17d: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

100. As shown in Figure 15, the time recorded by the clock on the computer running the TippingPoint LSM was 6:03 pm when the dynamic security policy discussed in relation to claim element 17c was received by the TippingPoint security gate segment 1. As detailed in relation to claim element 17c, this dynamic security policy specified that packets should be forwarded between Computer B (IP address of 172.15.3.5) and IP addresses within Network A in the range 192.168.137.2 – 192.168.137.3. Thus, this dynamic security policy was received by the TippingPoint security gate segment 1 at "a first time" of 6:03 pm, and said policy specifies "a first set of network addresses for which packets should be forwarded," as required by this claim element.

101. Thus, for at least the reasons above, it is my opinion that the TippingPoint system satisfies all requirements of claim element 17d of the '205 Patent.

102. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17d of the '205 Patent.

103. **Claim 17e: receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

104. Using the test setup described above in relation to Figure 7 and Figure 8, at 6:06 pm (as recorded by the clock on the computer running the TippingPoint PSM) a second dynamic security policy was communicated from the TippingPoint LSM, via the associated web server, to the TippingPoint security gateway segment 1. Figure 19 shows a screenshot from the TippingPoint LSM GUI of this second dynamic security policy, along with the computer clock confirming the second time of 6:06 pm.

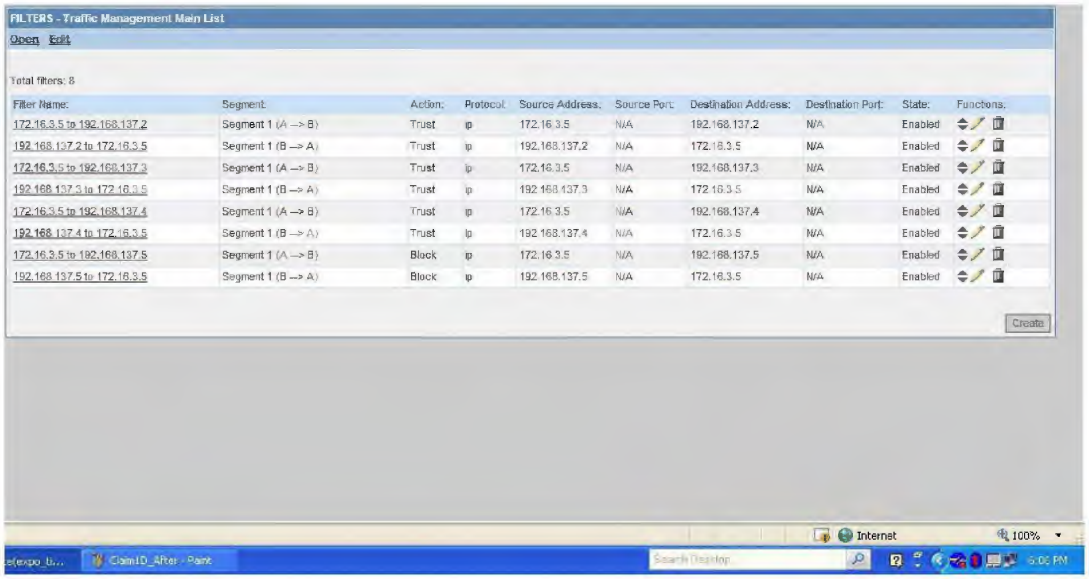


Figure 19. Screenshot of the second dynamic security policy

105. This second dynamic security policy modifies the set of network addresses for which packets should be forwarded. More specifically, the "Action" associated with rules 5 and 6 of the second dynamic security policy is set to "Trust," which causes packets that match the corresponding criteria to be forwarded; this is different from the previous dynamic security policy detailed in relation to claim elements 17c-d, in which the "Action" associated with rules 5 and 6 was set to "Block," causing packets that match the corresponding criteria to be dropped. Thus, the second dynamic security policy specified that packets should be forwarded between Computer B (IP address of 172.16.3.5) and IP addresses within Network A in the range 192.168.137.2 – 192.168.137.4, which is a larger range than that specified by the previous dynamic security policy under which packets associated with IP address 192.168.137.4 were dropped.

106. To demonstrate that the second dynamic security policy was installed, ping requests between Computer A (IP address 192.168.137.4) and Computer B (IP address 172.16.3.5)

were performed. Figure 20 shows a screenshot from Computer B that documents these ping requests: all four ping request packets were received by Computer A, and Computer B received four corresponding reply packets from Computer A.

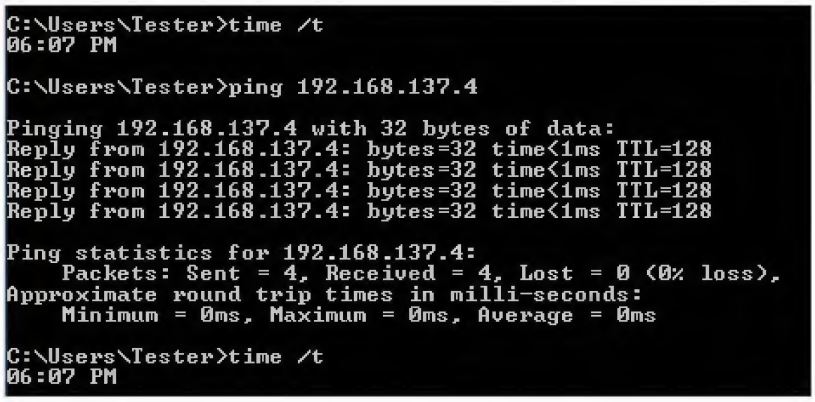


Figure 20. Screenshot of ping from Computer B to Computer A. Four packets were sent from Computer B to Computer A, and 4 replies were received by Computer A from Computer B.

107. The successful pings between Computer A and Computer B, which were blocked by the previous dynamic security policy as detailed in relation to claim element 17c, demonstrate that the second dynamic security policy has altered the set of network addresses for which packets should be forwarded such that said set now includes Computer A.

108. Thus, it has been demonstrated that the TippingPoint security gateway segment 1 received, at a second time of 6:06 pm, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded. Consequently, it is my opinion that the TippingPoint system satisfies all requirements of element 17e of the '205 Patent.

109. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17e of the '205 Patent.

110. **Claim 17f: receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after**

the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses. As detailed below, the TippingPoint system satisfies all requirements of this claim element.

111. Using the test setup described above in relation to Figure 7 and Figure 8, at 6:10 pm (as recorded by the clock on the computer running the TippingPoint PSM) a third dynamic security policy was communicated from the TippingPoint LSM, via the associated web server, to the TippingPoint security gateway segment 1. Figure 21 shows a screenshot from the TippingPoint LSM GUI of this second dynamic security policy, along with the computer clock confirming the second time of 6:10 pm.

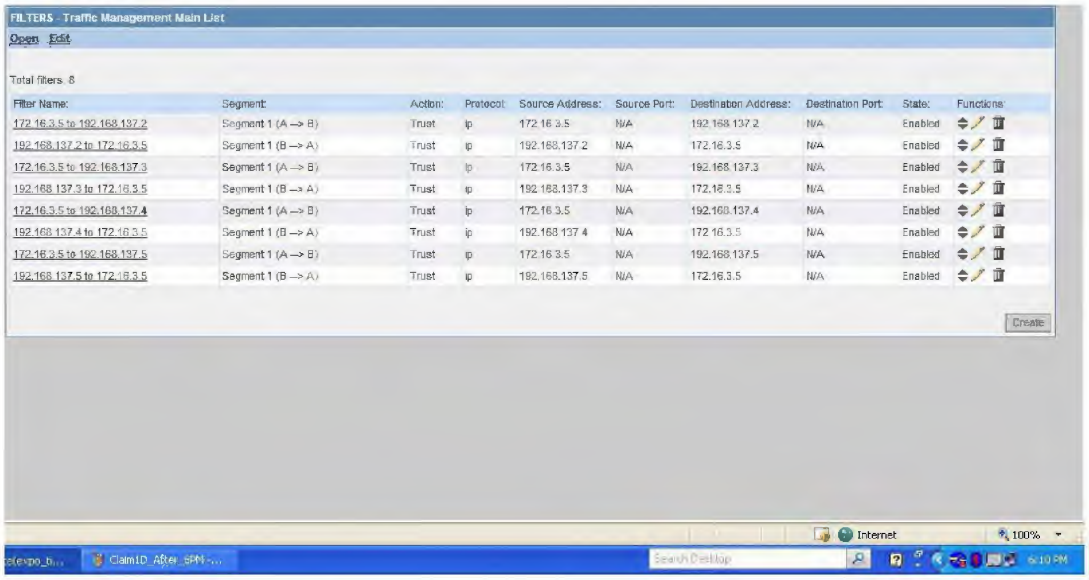


Figure 21. Screenshot of third dynamic security policy.

112. This third dynamic security policy modifies the set of network addresses for which packets should be forwarded. More specifically, the "Action" associated with rules 7 and 8 of

CENTRIPETAL-CSCO 087556

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 56

the second dynamic security policy is set to "Trust," which causes packets that match the corresponding criteria to be forwarded; this is different from the previous dynamic security policy detailed in relation to claim elements 17e, in which the "Action" associated with rules 7 and 8 was set to "Block," causing packets that match the corresponding criteria to be dropped. Thus, the third dynamic security policy specified that packets should be forwarded between Computer B (IP address of 172.16.3.5) and IP addresses within Network A in the range 192.168.137.2 – 192.168.137.5, which is a larger range than that specified by the previous dynamic security policy under which packets associated with IP address 192.168.137.5 were dropped.

113. In summary, as detailed in relation to claim elements 17c-f, three dynamic security policies were received by the TippingPoint security gate segment 1: the first, at a time of 6:03 pm, specified packets between Computer B and a set of IP addresses within Network A in the range 192.168.137.2 – 192.168.137.3 be forwarded; the second, at a time of 6:06 pm, specified packets between Computer B and a set of IP addresses within Network A in the range 192.168.137.2 – 192.168.137.4 be forwarded; and, the third, at a time of 6:10 pm, specified packets between Computer B and a set of IP addresses within Network A in the range 192.168.137.2 – 192.168.137.5 be forwarded. Therefore, three dynamic security policies were received by the TippingPoint security gate at three different times, specifying three different sets of IP addresses for which packets should be forward: the second time of 6:06 pm is after the first time of 6:03 pm; the third time of 6:10 pm is after the second time of 6:06 pm; the second set of network addresses included more network addresses than the first set; and, the third set of network addresses included more network addresses than the second

set. Thus, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 17f of the '205 Patent.

114. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17f of the '205 Patent.

115. **Claim 17g: receive packets associated with a network protected by the packet security gateway.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

116. As discussed in relation to the test setup, and as depicted in Figure 8, the TippingPoint security gateway segment 1 was located at an interface between Network A and Network B during the above-described demonstration. In this configuration, the TippingPoint security gateway segment 1 is protecting Network B from Network A. As demonstrated by the ping requests detailed above, the TippingPoint security gateway segment 1 receives packets associated with communication to and from Network B, which is protected by said security gateway. Thus, the TippingPoint system has been demonstrated to satisfy all requirements of element 17g of the '205 Patent.

117. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17g of the '205 Patent.

118. **Claim 17h: and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet**

transformation function other than forwarding or dropping the packets. As detailed below, the TippingPoint system satisfies all requirements of this claim element.

119. As detailed in relation to claim element 17a, the TippingPoint system performs "packet transformation functions" that satisfy both parties' proposed construction for this term.

120. As demonstrated in relation to claim elements 17c-h via ping requests, the TippingPoint system performs these packet transformation functions "on a packet by packet basis," according to the "plurality of dynamic security policies" upon packets that are "associated with the network protected" by TippingPoint security gateway segment 1.

121. As detailed in relation to claim element 17b, the TippingPoint system is able to perform packet transformation functions "other than forwarding or dropping the packets," as required by claim element 17h, at least because the logging of packets that attempt to access /etc/passwd constitutes a packet transformation function that satisfies this requirement. By way of a more specific example, a demonstration of this logging functionality performed using the test setup described in relation to Figure 7 and Figure 8 is described below.

122. Using the TippingPoint LSM and associated web server, the 0361:HTTP:Protected File Access (/etc/passwd) filter was configured to "Block + Notify + Trace" and installed on TippingPoint security gateway segment 1. A screenshot of the configuration used for this filter is shown in Figure 22 below; when configured as displayed, this filter redirects any packets that are attempting to access /etc/passwd to a log file and also performs tracing functionality, as discussed below.

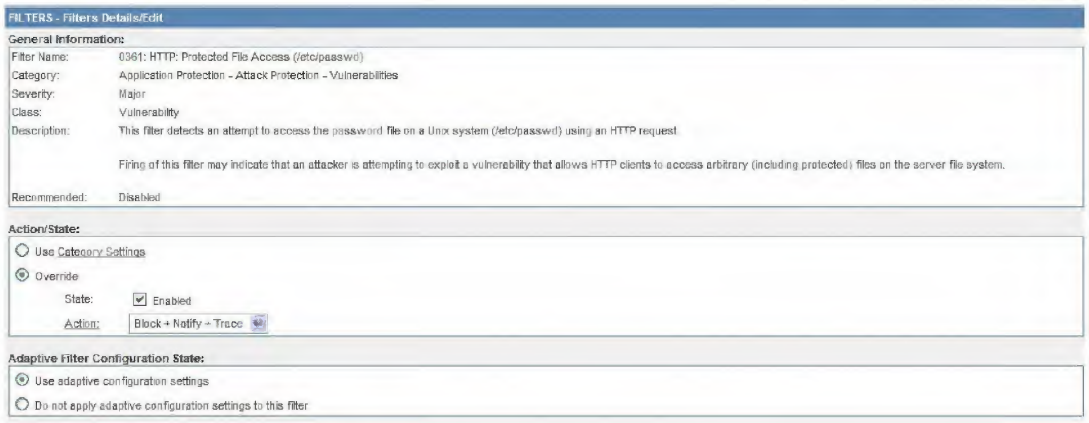


Figure 22. /etc/passwd filter, as configured to demonstrate packet transformation functions other than forwarding and dropping of packets.

123. In addition to installing the above-configured 0361:HTTP:Protected File Access (/etc/passwd) filter, all eight traffic management rules that were configured to "Trust" in the third dynamic security policy, which enables matching packets to be forwarded without inspection against other rules, were configured to "Allow." When set to "Allow," these traffic management rules themselves do not cause packets to be dropped, but the TippingPoint system still inspects packets that are permitted to be forwarded by the traffic management rules against other rules: i.e. setting the traffic management rules to "Allow" prevented any packets being dropped due to their associated IP addresses, but still enables packets to be subjected to other packet transformation operations if they match the criteria for other rules, such as the 0361:HTTP:Protected File Access (/etc/passwd). Figure 23 shows a screenshot of the traffic management rules used for demonstrating packet transformations other than forwarding or dropping.



Figure 23. Dynamic Security Policy. The "Allow" value in the "Action" field denotes the packets will be further inspected by the TippingPoint IPS.

124. With the above-described rules installed on TippingPoint security gateway segment 1, "ncat" was used to open a connection between Computer A and Computer B. An HTTP server was hosted on port 8000 of Computer B, and Computer A was used to attempt to access /etc/passwd file using a HTTP GET request. Figure 24 shows a screen shot from Computer B showing the command used to host the web server. Figure 25 shows a screenshot from Computer A attempting to access Computer B's /etc/passwd file using a HTTP GET request.

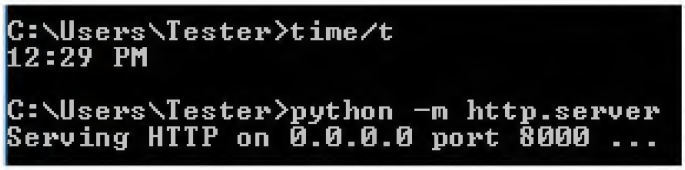


Figure 24. Hosting the HTTP website on Computer B.



Figure 25. Sending "GET /etc/passwd" request from Computer A (192.168.137.4) to Computer B (172.16.3.5) on port 8000.

125. The resulting logs stored on the TippingPoint system were accessed using the TippingPoint LSM GUI. As shown in Figure 26, the HTTP GET request to the file protected by the 0361:HTTP:Protected File Access (/etc/passwd) filter was blocked and logged in the Block Log.



Figure 26. Screenshot from the TippingPoint LSM GUI showing the Block Log, which lists packets that were not forwarded to their intended destination.

126. In addition to being logged, the HTTP GET request packet was also traced, and the trace of said packet was downloaded from the Block Log (by clicking the icon in the "Packet Trace" column). Figure 27 shows the contents of the trace when viewed using Wireshark[39] which includes various information regarding the packet, such as the source and destination IP addresses, as well as the packet data content: e.g., the ASCII characters that make up the "GET /etc/passwd HTTP/1.1" request are clearly visible.

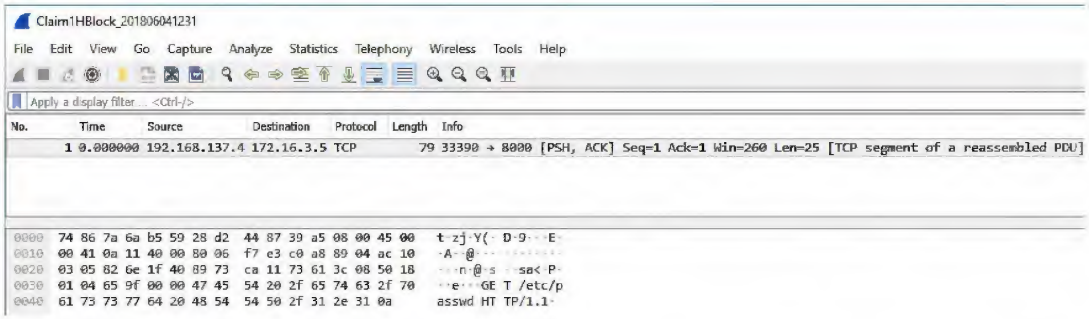


Figure 27. Packet information logged by the TippingPoint system. For example, the ASCII characters "GET /etc/passwd HTTP/1.1" can be seen in the lower right section of this figure.

[39] Wireshark is a network analysis computer program. See, for example, https://www.wireshark.org.

CENTRIPETAL-CSCO 087562

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 62

127. The above testing demonstrates that the TippingPoint system can apply "at least one packet transformation function other than forwarding or dropping the packets," at least because logging and tracing constitute such packet transformation functions. Hence, the above demonstration, in conjunction with the testing described in relation to claim elements 17a-g, demonstrate that all requirements of claim element 17h are satisfied by the TippingPoint system.

128. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 17h of the '205 Patent.

129. As detailed above, it is my opinion that all requirements of each and every element of claim 17 of the '205 Patent are anticipated by the TippingPoint system. Consequently, for at least the reasons above, it is my opinion that claim 17 of the '205 Patent is anticipated by the TippingPoint system.

3. CLAIM 33

130. **Claim 33a: One or more non- transitory computer readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

131. For at least the reasons detailed in relation to claim 17 above, the TippingPoint system comprises "packet security gateways" that are associated with a "security policy management server," where each of these terms is interpreted according to the relevant claim constructions.

132. Furthermore, the TippingPoint IPS computer contains a hard drive, which constitutes a "non-transitory computer readable media"; and, this hard drive stores programs and data resources required to enable the TippingPoint IPS to operate, which constitute "instructions stored thereon" for causing the packet security gateways to function.

133. Thus, for at least the reasons above, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33a of the '205 Patent.

134. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33a of the '205 Patent.

135. **Claim 33b: receive a plurality of dynamic security policies from the security policy management server.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

136. As detailed in relation to claim element 17b above, the TippingPoint security gateway segments receive "a plurality of dynamic security policies" from the TippingPoint LSM and associated web server, which constitute a "security policy management server," where said "dynamic security policies" satisfy the relevant claim constructions proposed by both parties.

137. Thus, for at least the reasons detailed in relation to claim 17, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33b of the '205 Patent.

138. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33b of the '205 Patent.

139. **Claim 33c: receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which**

packets should be forwarded should be dropped. As detailed below, the TippingPoint system satisfies all requirements of this claim element.

140. Exponent has demonstrated that the TippingPoint system satisfies all requirements of this claim element, as set forth in relation to claim element 17c above. Thus, for at least the same reasons as detailed in relation to claim element 17, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33c of the '205 Patent.

141. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33c of the '205 Patent.

142. **Claim 33d: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

143. Exponent has demonstrated that the TippingPoint system satisfies all requirements of this claim element, as set forth in relation to claim element 17d above. Thus, for at least the same reasons as detailed in relation to claim element 17, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33d of the '205 Patent.

144. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33d of the '205 Patent.

145. **Claim 33e: receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

146. Exponent has demonstrated that the TippingPoint system satisfies all requirements of this claim element, as set forth in relation to claim element 17e above. Thus, for at least the same

reasons as detailed in relation to claim element 17, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33e of the '205 Patent.

147. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33e of the '205 Patent.

148. **Claim 33f: receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

149. Exponent has demonstrated that the TippingPoint system satisfies all requirements of this claim element, as set forth in relation to claim element 17f above. Thus, for at least the same reasons as detailed in relation to claim element 17, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33f of the '205 Patent.

150. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33f of the '205 Patent.

151. **Claim 33g: receive packets associated with a network protected by the packet security gateway.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

152. Exponent has demonstrated that the TippingPoint system satisfies all requirements of this claim element, as set forth in relation to claim element 17g above. Thus, for at least the same

reasons as detailed in relation to claim element 17, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33g of the '205 Patent.

153. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33g of the '205 Patent.

154. **Claim 33h: and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets**. As detailed below, the TippingPoint system satisfies all requirements of this claim element.

155. Exponent has demonstrated that the TippingPoint system satisfies all requirements of this claim element, as set forth in relation to claim element 17h above. Thus, for at least the same reasons as detailed in relation to claim element 17, it is my opinion that the TippingPoint system satisfies all requirements of claim element 33h of the '205 Patent.

156. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 33h of the '205 Patent.

D. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF CHECK POINT R75

157. The Check Point R75 security gateway (SG) product[40] performs the functionality of a packet security gateway, and the Check Point R75 security management server (SMS)

[40] See "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

product[41] performs the functionality of security policy management server. An illustration of how the R75 SG and R75 SMS fit into a typical network architecture is shown in Figure 28.

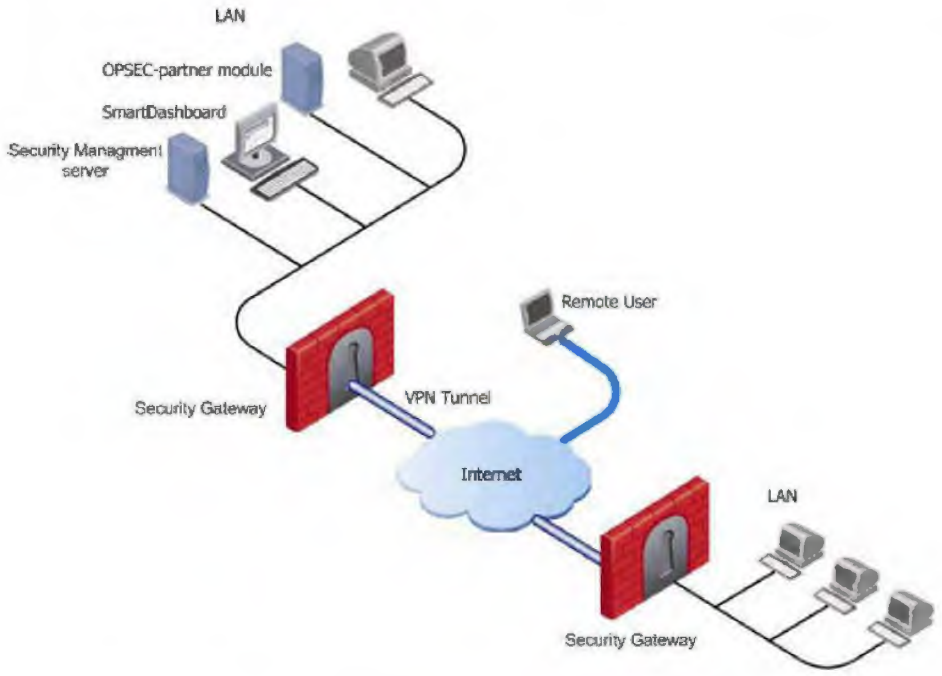


Figure 28. Illustration of a typical deployment consisting of two security gateways and a security management server (configurable using the "SmartDashboard" GUI).[42]

158. The Check Point R75 system was commercially available to purchase before the priority date of the '205 Patent. For example:

a. The Check Point Release Map indicates that R75 was available for upgrade in December 2010. (Check_Point_R7x_xx_Releases_Maps_May_2017.pdf).

b. The splash screen on the Check Point R75 software indicates a copyright date "© 2010". (R75 Splash Screen).

c. The Firewall, SecurePlatform, and Security Management Server Administration Guides for CheckPoint R75 are dated December 15, 2010 and all show a revision

[41] See "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).
[42] See p. 10, "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).

history stating that the document was first released on December 15, 2010. (CP_R75_Firewall_AdminGuide; CP_R75_SecurePlatform_AdminGuide; CP_R75_SecurityManagement_AdminGuide).

d. The R75 Installation and Upgrade Guide dated March 24, 2011 indicates that the first release of the document was on December 15, 2010. (CP_R75_Installation_and_Upgrade_Guide).

e. On January 2, 2011, a YouTube video was posted by Check Point Support Channel titled "How to Install R75 Multi Domain Management Server". (https://www.youtube.com/watch?v=NZ5jXCKDx2Y).

f. On February 8, 2011, Check Point issued a press release noting the release of R75 and stated "Check Point R75 is available immediately." WayBack Machine March 3 2011 capture of Check Point Website (https://web.archive.org/web/20110303142320/http:/www.checkpoint.com:80/press/2011/CheckPoint-R75-02.08.11.html).

g. On February 13, 2011, Check Point's website advertised Check Point R75 and provided a link for customers to "receive more information on Release R75 Network Security Suite." February 13 2011 capture of Check Point website (https://web.archive.org/web/20110213040305/http:/www.checkpoint.com:80/campaigns/r75/index.html).

h. At least one brochure that Centripetal produced shows that Check Point R75 was being offered for sale in 2011. CENTRIPETAL0045961.

159. For at least the reasons detailed below, it is my opinion that the Check Point R75 system enabled a person of ordinary skill in the art to practice each and every element of Claims 17

and 33 of the '205 Patent, and thus the Check Point R75 system anticipates these claims. In addition to the analysis presented herein, further discussion of relevant testing is described in Appendix C, which I incorporate by reference.

1. TEST CONFIGURATION WITH CHECK POINT R75

160. Exponent procured the Check Point R75 SMS product and installed it on a 32-bit PC-compatible Dell Latitude E6400 computer using the "Check_Point_R75.Splat.iso" DVD ISO image.[43]

161. Exponent also procured the Check Point R75 SG product and installed it on two 32-bit PC-compatible Dell PowerEdge 1750 computers using the "Check_Point_R75.Splat.iso" DVD ISO image.

162. The SMS and SGs were installed in a "Distributed Deployment" configuration (see Figure 28) wherein the SMS is installed on a different machine than the SGs.

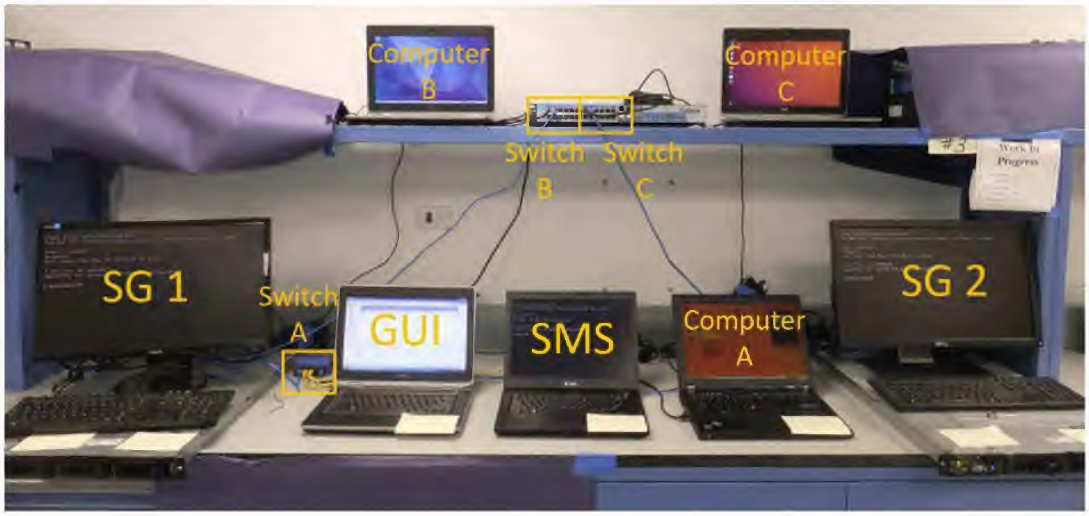


Figure 29. Photograph of test network used as part of the claim analysis that shows a hardware installation of two security gateways (SG 1 and SG 2), one security management server (SMS) with its associated SmartDashboard graphical user

[43] According to the Check Point website, DVD installation material was available in December 2010 (see https://supportcenter.Check Point.com/supportcenter/) and the installation procedure for the Firewall and Security Management Server is documented in the "R75 Installation and Upgrade Guide."

CENTRIPETAL-CSCO 087570

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 70

interface (GUI). Computers A, B, and C reside in three separate networks connected by the security gateways. Each network has one switch to route traffic

163. Figure 29 shows the physical layout of the hardware, including the two security gateways, the security management server, the SmartDashboard interface, three switches, and three computers for sending and receiving traffic.

164. The test network shown in Figure 29 includes three subnetworks (subnets). Only two of these subnets are required to demonstrate how the Check Point R75 system satisfies the requirements of Claims 17 and 33.

165. The first subnet is called "Network A" and includes IP addresses in the range from 192.168.1.0 through 192.168.1.255. Network traffic internal to Network A is communicated via a TRENDent TE100-S5 switch (Switch A).

166. The second subnet is called "Network B" and includes IP addresses in the range from 172.16.1.0 through 172.16.1.255. Network traffic internal to Network B is communicated via a VLAN on a HP ProCurve 2510-24 that uses the ProCurve Ethernet ports numbered 1—12 (Switch B).

167. Network A and Network B are connected by an R75 SG, which we refer to as "Security Gateway 1" or "SG 1." This security gateway is also referred to as "cpgateway1" in the SmartDashboard GUI.

168. The test network shown in Figure 29 also includes a third subnet called "Network C" that includes IP addresses in the range from 10.0.42.0 through 10.0.42.255. Network traffic internal to Network C is communicated via a VLAN on a HP ProCurve 2510-24 that uses the ProCurve Ethernet ports numbered 13–24 (Switch C). Network A and Network C are connected by an R75 SG called "Security Gateway 2" or "SG 2." This security gateway is also referred to as "cpgateway2" in the SmartDashboard GUI. However, only Security

Gateway 1 is used to illustrate how the R75 system performs the method of Claims 17 and 33.[44]

169. Figure 30 shows the schematic layout of the networks. Network A includes the R75 SMS (the security policy management server) along with another computer called "Computer A." Network B includes another computer called "Computer B." Network C includes another computer called "Computer C." Security Gateway 1 protects Network B from Network A. Security Gateway 2 protects Network C from Network A.

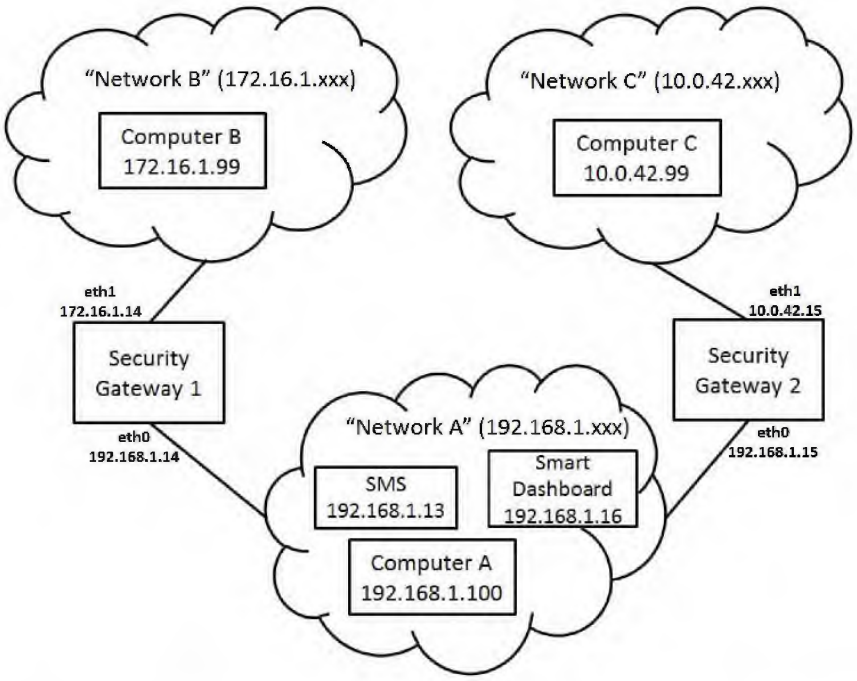


Figure 30. Schematic of test network (see Figure 29) architecture, including the static IP addresses of each element. Each network has its own subnet. SG 1 protects Network B from Network A. SG 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (eth0 and eth1), which are used to pass traffic between networks.

[44] Prior to Plaintiffs' Centripetal Networks, Inc.'s Identification of Asserted Claims, dated June 22nd, 2018, claims 91, 93, and 95 were also at issue in this litigation; these claims required a third network, and Network C was used for demonstrating that these claims were also satisfied by the TippingPoint system.

2. CLAIM 17

170. **Claim 17a: A system, comprising: security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to.** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

171. The '205 Patent states that "[a]s used herein, a security policy management server includes any computing device configured to communicate a dynamic security policy to a packet security gateway."[45] I understand, however, that the parties have agreed that the term "security policy management server" is to be construed as "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway,"[46] and I have applied this claim construction throughout my analysis. The Check Point R75 system comprises a security policy management server, for at least the following reasons.

172. The Check Point R75 system includes the Check Point R75 security management server (SMS). According to the Check Point R75 Security Management Server Administration Guide, the "*Security Management server* is the component that manages the database and policies, and downloads policies to gateways."[47] This guide also states that "[t]he Security Management server manages the gateways and allows remote users to connect securely to the corporate network." [48] It goes on to state that "SmartDashboard may be installed on the Security Management server or on any other machine." SmartDashboard is the "set of GUI

[45] '205 Patent, at 4:37-40.
[46] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.
[47] See p.11"Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).
[48] See p.10"Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).

applications used to manage different aspects of the corporate network" referred to as "SmartConsole," which is "used to create, edit and install policies," and allows for the management of objects that "represent actual network components such as gateways, servers and networks."[49] Thus, the Check Point R75 system includes a graphical user interface (GUI) with which dynamic security policies may be managed and communicated to the Check Point R75 security gateways. Therefore, the Check Point R75 system includes "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway," as required by the claim construction of "security policy management server." Moreover, although I have applied the agreed upon claim constructions throughout my analysis, the Check Point R75 system also satisfies the definition for "security policy management server" stated within the '205 Patent, at least because the laptop running the security management server (SMS) with its associated SmartDashboard graphical user interface (GUI) constitutes a "computing device configured to communicate a dynamic security policy to a packet security gateway," which is broader than the agreed upon construction.

173. The '205 Patent states that "[a]s used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation on the packets."[50] I understand, however, that the parties have agreed that the term "packet security gateway" is to be construed as "a gateway computer configured to receive packets and perform a packet transformation function on the packets,"[51] and I have applied this claim construction throughout my analysis.

---

[49] See p.11"Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).
[50] '205 Patent, at 4:33-35.
[51] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.

174. I also understand that there is a dispute regarding the construction of the term "packet transformation function." More specifically, Plaintiffs have proposed that this term be construed as "function that transforms packets from one state to another" while Defendants have proposed "an operation performed on a packet specified by the dynamic security policy, such as forward or drop."[52] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R75 system comprises "one or more packet security gateways," as detailed below.

175. According to the Check Point R75 documentation,[53] "[a] Security Policy consists of an ordered set of rules, collectively known as the Rule Base…The Security Gateway inspects packets and applies rules in a sequential manner. When a Security Gateway receives a packet from a connection, it inspects the packet and applies the first rule in the Rule Base, then the second rule and so on. Once all elements in a given rule match the information contained the packet (source, destination, service, etc.), the Security Gateway stops the inspection and immediately applies that rule. If no applicable rule is found in the Rule Base, the traffic is automatically blocked." This is exemplified in the test setup shown in Figure 29, which includes two separate packet security gateways wherein each security gateway can be programmed independently to follow its own set of filtering rules. In this test setup Network A and Network B are connected by security gateway 1. This security gateway is a "packet security gateway" as it receives all packets that pass between these two networks. Upon receiving packets, the computer within the Check Point R75 SG (i.e. SG1) applies rules according to the currently enforced security policy. Thus, the Check Point R75 system

[52] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.
[53] See pp. 10–11, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

includes "a gateway computer configured to receive packets" as required by the agreed upon construction for "packet security gateway."

176. As discussed above, there is a dispute as to the interpretation of "packet transformation function." However, the Check Point R75 system satisfies both parties proposed construction for this term for at least the reasons herein. Plaintiff's proposed construction of "packet transformation function" requires a function that "transforms one or more packets from one state to another." Although Plaintiff has not provided an explicit definition for transforming "from one state to another," the intrinsic evidence cited to by Plaintiff in support of their proposed construction includes example embodiments in which packets are forwarded or dropped depending upon parameters of the packet such as the origination IP address. Thus, under Plaintiff's proposed construction, forwarding or dropping of packets constitutes transforming a packet from one state to another, and hence forwarding or dropping satisfy Plaintiff's construction of "packet transformation function." Similarly, Defendants' proposed construction for "packet transformation function" explicitly includes the operations "forward or drop," and hence forwarding or dropping also satisfy Defendant's proposed construction for this term. As detailed below in relation to other claim elements, the Check Point R75 can perform a variety of functions upon the received packets, depending upon the rules within the current policy and parameters of the received packets, including but not limited to: forwarding packets to their intended address; forwarding packets to an address other than their intended address; dropping packets; logging or otherwise monitoring packets. Therefore, the Check Point R75 system satisfies both parties' proposed construction for "packet transformation function."

177. Therefore, for at least the reasons above, each of the Check Point R75 SGs constitutes "a gateway computer configured to receive packets and perform a packet transformation function on the packets," and hence the Check Point R75 system comprises "one or more packet security gateways," as required by this claim element as construed by both parties.

178. **Claim 17b: receive a plurality of dynamic security policies from the security policy management server.** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

179. I understand there is a dispute regarding the construction of the term "dynamic security policy." More specifically, Plaintiff has proposed that this term be construed as "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets," while Defendants have proposed that this term be construed as "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria".[54] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R75 system satisfies all requirements of this claim element, for at least the reasons detailed below.

180. The Check Point R75 documentation explains that "[t]he Security Management Server enables administrators to enforce security policies," and that this is accomplished by administrators defining a security policy Rule Base. As stated above in relation to claim element 17a "[a] Security Policy consists of an ordered set of rules, collectively known as the Rule Base…The Security Gateway inspects packets and applies rules in a sequential manner.

[54] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

When a Security Gateway receives a packet from a connection, it inspects the packet and applies the first rule in the Rule Base, then the second rule and so on."[55] Thus, Check Point R75 system's Security Policies are dynamic security policies.

181. According to the Check Point R75 documentation, these security policies can be installed on selected security gateways using the security management server.[56] This has been exemplified in the setup, shown in Figure 29 above, wherein tests have demonstrated how the Check Point R75 system performs the requirements of claim element 17b by receiving two rules and three security policies from the security management server. This is described in greater detail below in relation to claim element 17c.

182. For at least the reasons set forth in relation to claim element 17a, the Check Point R75 Security Management Server (SMS) comprises a "security policy management server," as required by this claim element and the associated claim construction agreed upon by both parties; and each Check Point R75 Security Gateway (SG) constitutes a "packet security gateway," as required by this claim element and the associated claim constructions.

183. Thus, as explained above, the Check Point R75 SGs receive a plurality of dynamic security policies from the Check Point R75 SMS, and this satisfies all requirements of claim element 17b of the '205 Patent.

184. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 17b of the '205 Patent

185. **Claim 17c: receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets**

---

55 See pp. 10–11, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

56 See, generally, pp. 28–29, "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010); see also p. 9 "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010): "Granular security policy control is possible by applying specific rules to specific gateways."

associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped. As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

186. I understand there is a dispute regarding the construction of the term "rule." More specifically, Plaintiff has proposed that this term be construed as "condition or set of conditions that when satisfied cause a specific action to occur," while Defendants have proposed that this term be construed as "(i) packet-identifying criteria and (ii) a function to be performed on the identified packets."[57] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R75 system satisfies all requirements of this claim element, for at least the reasons detailed below.

187. Using the Check Point R75 system, a security policy with two explicit rules was implemented. The first explicit rule allowed any traffic from Computer B to be forwarded. The second explicit rule allowed any traffic from a range of IP addresses to be forwarded. Initially, this IP address range was set to be 192.168.1.101 – 192.168.1.102, which does not include any devices in the test system. Figure 31 shows a screenshot of this security policy from the SmartDashboard GUI.

[57] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

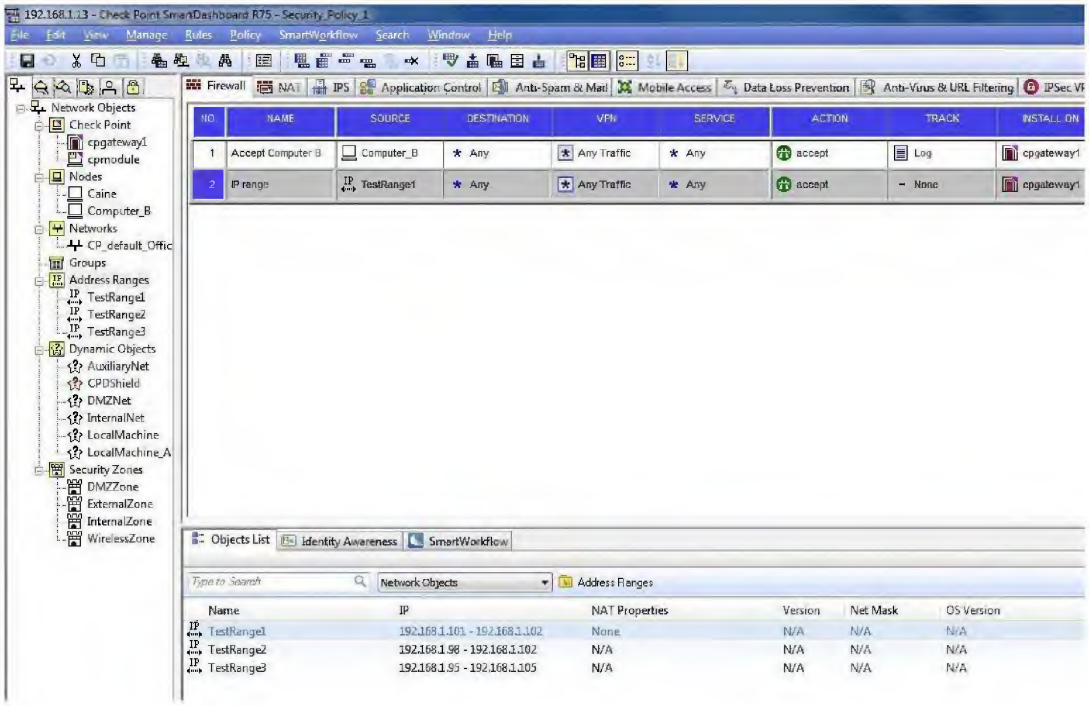


Figure 31. Screenshot of SmartDashboard GUI showing security policy with two explicit rules. The range of IP addresses allowed by the second rule is 192.168.1.101 – 192.168.1.102.

188. These rules satisfy both the proposed claim constructions. For example, these rules contain a "condition or set of conditions" based upon the IP addresses associated with received packets, and cause "a specific action to occur" (i.e. forward) when packets satisfy said condition or set of conditions: thus, Plaintiff's proposed construction is satisfied. Also, for these rules the associated IP addresses of received packets are used as a "packet-identifying criteria" and "a function" (i.e. forward) is "performed on the identified packets": thus, Defendants' proposed construction is also satisfied.

189. Check Point R75 also uses implied rules, which are included in the security policy. Implied rules enable certain connections to occur to and from the security gateways using a variety of different services and always include the Last Implied Rule, or "the default rule,

which typically rejects all packets without logging."[58] The Last Implied Rule thus will cause packets from IP addresses outside the explicit range of allowed IP addresses to be dropped; or, more generally, cause packets that do not satisfy the criteria of at least one rule in the current security policy to be dropped. A Cleanup Rule can also be included, which, like the Last Implied Rule, drops all traffic that is not permitted by the previous rules and allows logging.[59] We did not include a Cleanup Rule in our policy.

190. As shown in the screenshot in Figure 32, this policy was installed on Security Gateway 1 (The hostname of Security Gateway 1 is "cpgateway1," as seen on the right side of Figure 31).

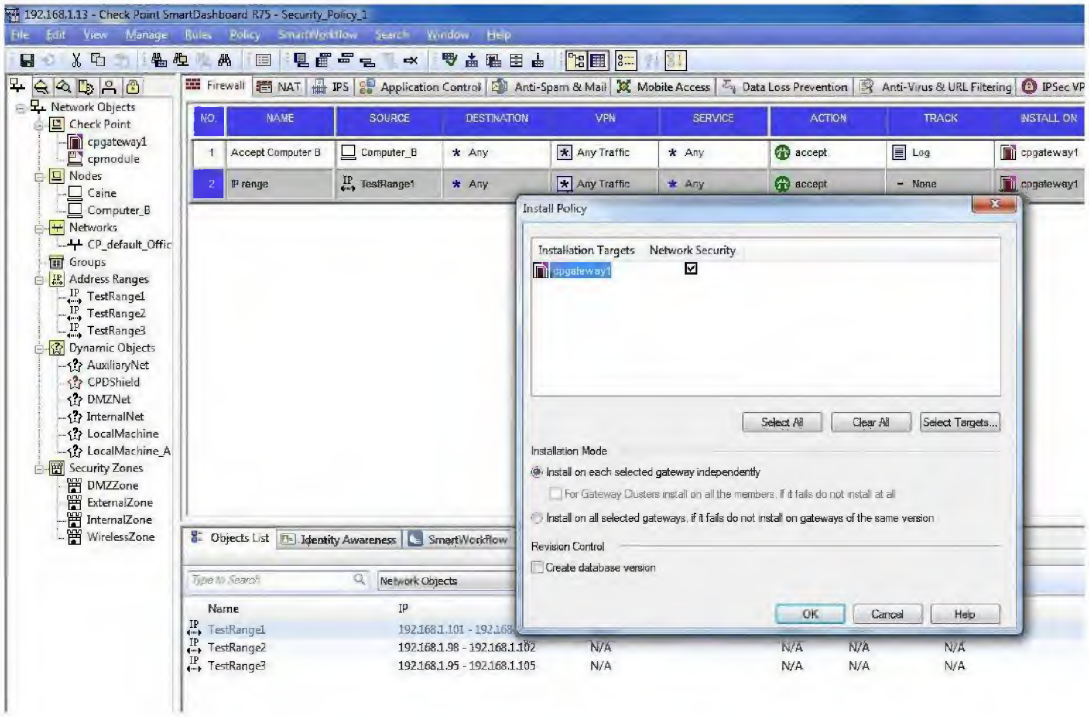


Figure 32. Installation of security policy on Security Gateway 1

58 See p. 11, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).
59 See pp. 11–12, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

CENTRIPETAL-CSCO 087581

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 81

191. The security policy installation proceeded to completion with no errors (see Figure 33).[60]

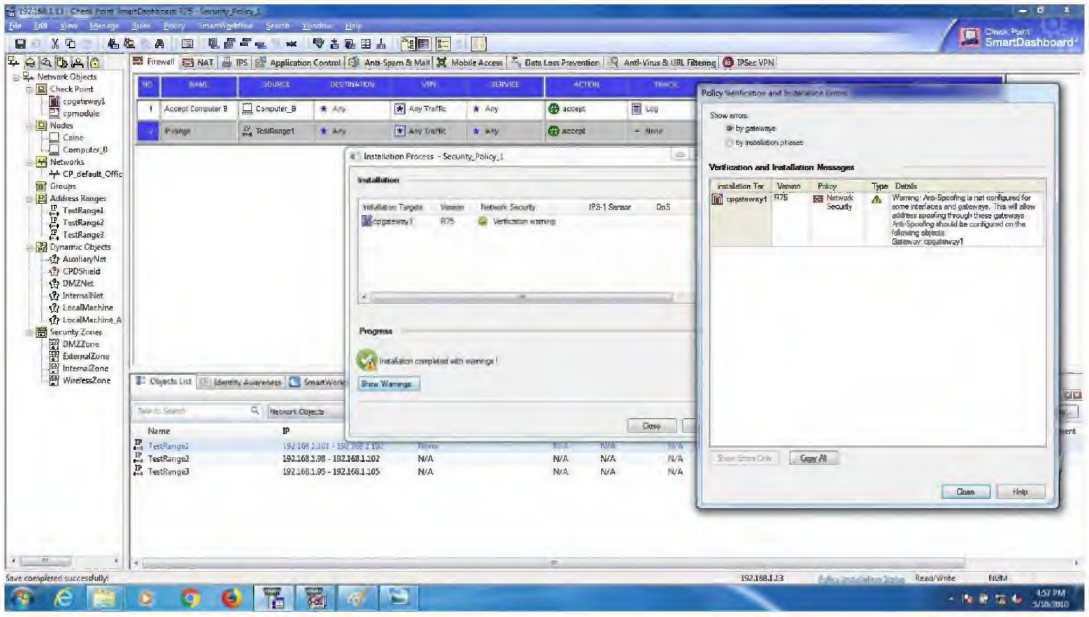


Figure 33. Dialog boxes indicating that the installation of the security policy completed. The clock in the lower right corner of the figure shows that this policy was installed around 4:57 pm.

192. To demonstrate the operation of the security policy on Exponent's test setup, an attempt was made to send traffic from Computer A, whose IP address is outside the allowed range of Rule 2, to Computer B through Security Gateway 1.

193. First, an attempt was made to ping Computer B from Computer A (see Figure 34). Using tcpdump to monitor traffic on interface eth0 of SG 1, incoming packets from Computer A (192.168.1.100) were observed, as shown in Table 12 below.

16:58:24.005864 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)
16:58:25.014620 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)

Table 12. Incoming traffic from Computer A observed via the "tcpdump" utility on SG 1. No ICMP echo reply was observed.

194. These packets were dropped by SG 1 before they reached Computer B (172.16.1.99).

[60] The installation completed with no errors and one warning that "anti-spoofing" was not configured. Anti-spoofing, which is not configured for our test setup, is described, for example, on page 14 of the "Check Point R75 Firewall Administration Guide" document.

CENTRIPETAL-CSCO 087582

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 82

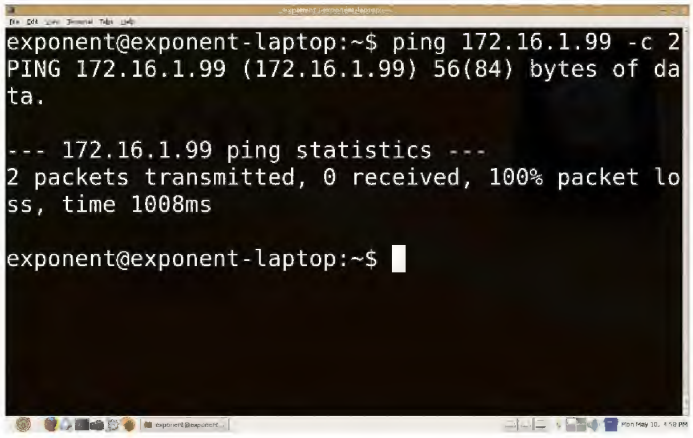


Figure 34. Screenshot of ping from Computer A ("exponent-laptop") to Computer B (172.16.1.99) indicating 100% packet loss, demonstrating that the security gateway dropped the packets

195. As a second demonstration of the security policy functionality of Exponent's test setup, the computer program "netcat" was used to attempt to establish a connection between Computer A and Computer B. While listening with "netcat" on Computer B, an attempt was made to send a test packet of text ("test_packet") from Computer A (see Figure 35 and Figure 36). The packet was not received by Computer B.

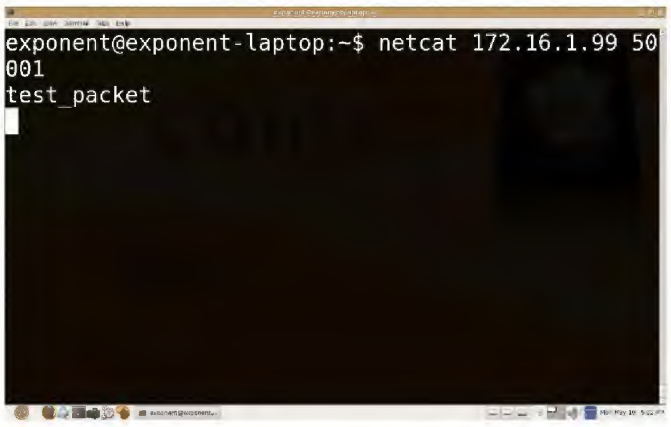


Figure 35. Sending packet of text ("test_packet") from Computer A ("exponent-laptop") to Computer B (172.16.1.99) on port 50001.

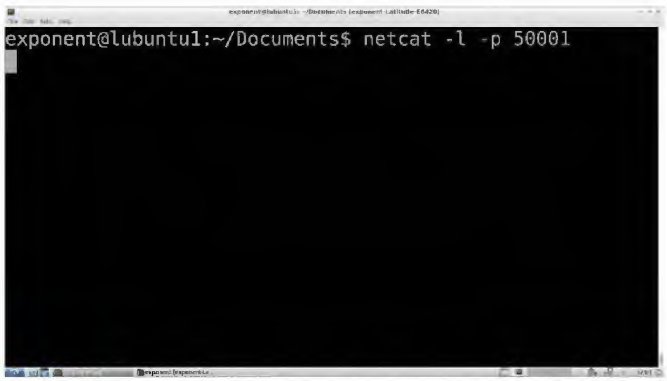


Figure 36. Listening for a packet of text ("test_packet") from Computer A on port 50001 on Computer B. No packet was received.

196. Thus, Exponent's test setup of the Check Point R75 system has demonstrated a security policy that includes at least one rule specifying a set of network addresses for which associated packets should be forwarded (explicit Rule 1 and Rule 2) and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped (the Last Implied Rule). Based on the analysis of network traffic and the Check Point documentation, the Last Implied Rule drops all packets associated with network addresses outside the set of network addresses for which packets should be forwarded.

197. Thus, for at least the reasons above, it is my opinion that the Check Point R75 system satisfies all requirements of element 17c of the '205 Patent.

198. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 17c of the '205 Patent.

199. **Claim 17d: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

200. At 4:57 pm, as recorded by the clock (see Figure 33) on the SmartDashboard GUI, Security Gateway 1 received the dynamic security policy outlined in relation to claim element 17c above. This policy specified a set of network addresses for which packets should be forwarded: 192.168.1.101 – 192.168.1.102.

201. Thus, for at least the reasons above, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 17d of the '205 Patent.

202. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 17d of the '205 Patent.

203. **Claim 17e: receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

204. As shown in Figure 37, at 5:04 pm (as recorded by the clock on the SmartDashboard GUI), Security Gateway 1 received a security policy with a second set of network addresses for which packets should be forwarded, contained in Rule 2: 192.168.1.98 – 192.168.1.102. This range includes more network addresses than the range in the security policy discussed in relation to claim element 17d. The time at which this second security policy was installed was later than the time at which the first security policy was installed.

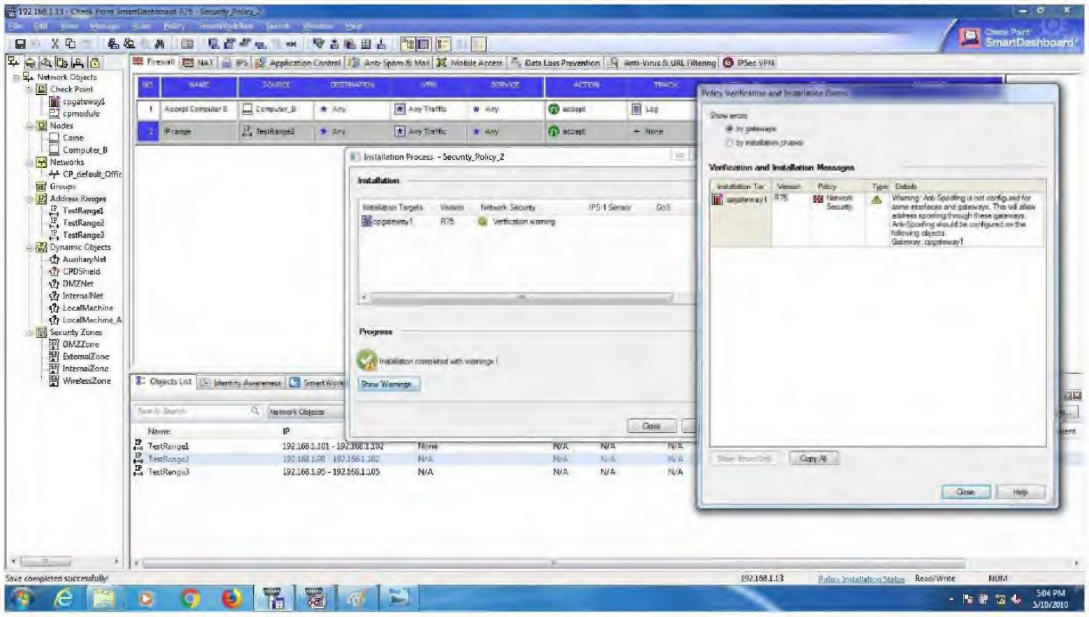


Figure 37. Screenshot of SmartDashboard GUI showing that a dynamic security policy specifying a second set of network addresses for which packets should be forwarded was received by Security Gateway 1 at 5:04 pm.

205. The range of network addresses that should be forwarded according to Rule 2 in this second security policy includes the address of Computer A.

206. To demonstrate the operation of Rule 2, an attempt was made to send packets from Computer A to Computer B. Rule 2 should allow forwarding of this traffic.

207. First, an attempt was made to ping Computer B from Computer A (see Figure 38). Using tcpdump to monitor traffic on interface eth0 of SG 1, request packets from Computer A (192.168.1.100) and response packets from Computer B (172.16.1.99) were observed, shown below in Table 13, indicating that SG 1 was forwarding packets from Computer A to Computer B, as required by Rule 2:

17:04:37.877141 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)
17:04:37.878478 172.16.1.99 > 192.168.1.100: icmp: echo reply
17:04:38.876155 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)
17:04:38.876775 172.16.1.99 > 192.168.1.100: icmp: echo reply

Table 13. Traffic between Computer A and Computer B as observed via the "tcpdump" utility on SG1.

CENTRIPETAL-CSCO 087586

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 86

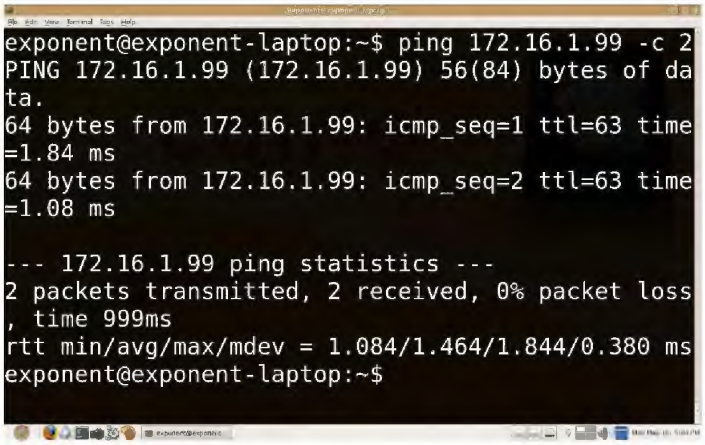


Figure 38. Screenshot of ping from Computer A ("exponent-laptop") to Computer B (172.16.1.99) indicating 0% packet loss, demonstrating that the security gateway forwarded the packets.

208. Also, "netcat" was used to establish a connection between Computer A and Computer B. While listening with "netcat" on Computer B, an attempt was made to send a test packet of text ("test_packet") from Computer A (see Figure 39 and Figure 40). The packet was received by Computer B.

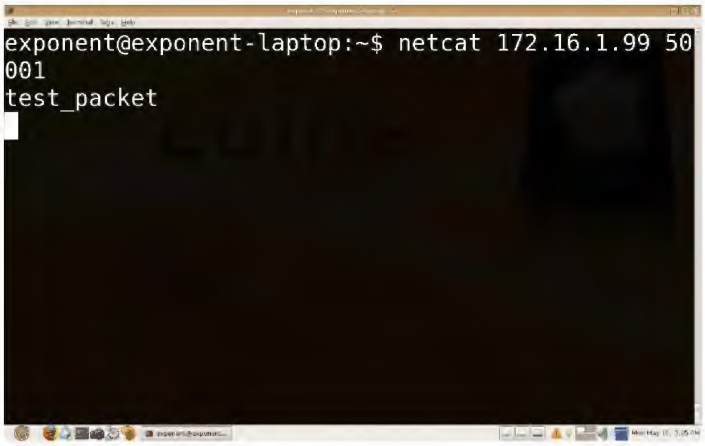


Figure 39. Sending packet of text ("test_packet") from Computer A ("exponent-laptop") to Computer B (172.16.1.99) on port 50001.

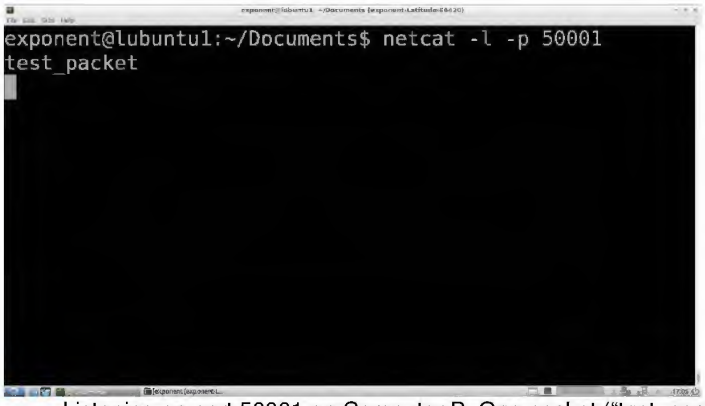


Figure 40. Listening on port 50001 on Computer B. One packet ("test_packet") was received from Computer A

209. In addition, using tcpdump to monitor traffic on interface eth0 of SG 1, traffic from Computer A (192.168.1.100) to Computer B (172.16.1.99) and back was observed, shown in Table 14 below, indicating that SG 1 was forwarding packets from Computer A to Computer B, as required by Rule 2:

17:05:29.842216 192.168.1.100.35948 > 172.16.1.99.50001: P 1:13(12) ack 1 win 46 <nop,nop,timestamp 64608257 2561232124> (DF)
17:05:29.842726 172.16.1.99.50001 > 192.168.1.100.35948: . ack 13 win 227 <nop,nop,timestamp 2561236191 64608257> (DF)

Table 14. Traffic between Computer A and Computer B as observed via the "tcpdump" utility on SG1

210. Thus, it has been demonstrated that a dynamic security policy specifying a set of network addresses for which packets should be forwarded was received. Based on the analysis of network traffic and the Check Point documentation, Rule 2 of this security policy allows packets to be forwarded through the security gateway. Consequently, it is my opinion that the Check Point R75 system satisfies all requirements of element 17e of the '205 Patent.

211. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 17e of the '205 Patent.

212. **Claim 17f: receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after**

CENTRIPETAL-CSCO 087588

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 88

the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses. As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

213. As shown in Figure 41, at 5:08 pm (as recorded by the clock on the SmartDashboard GUI), Security Gateway 1 received a security policy with a third set of network addresses for which packets should be forwarded: 192.168.1.95 – 192.168.1.105. This range includes more network addresses than the range in the security policy discussed in relation to claim element 17e.

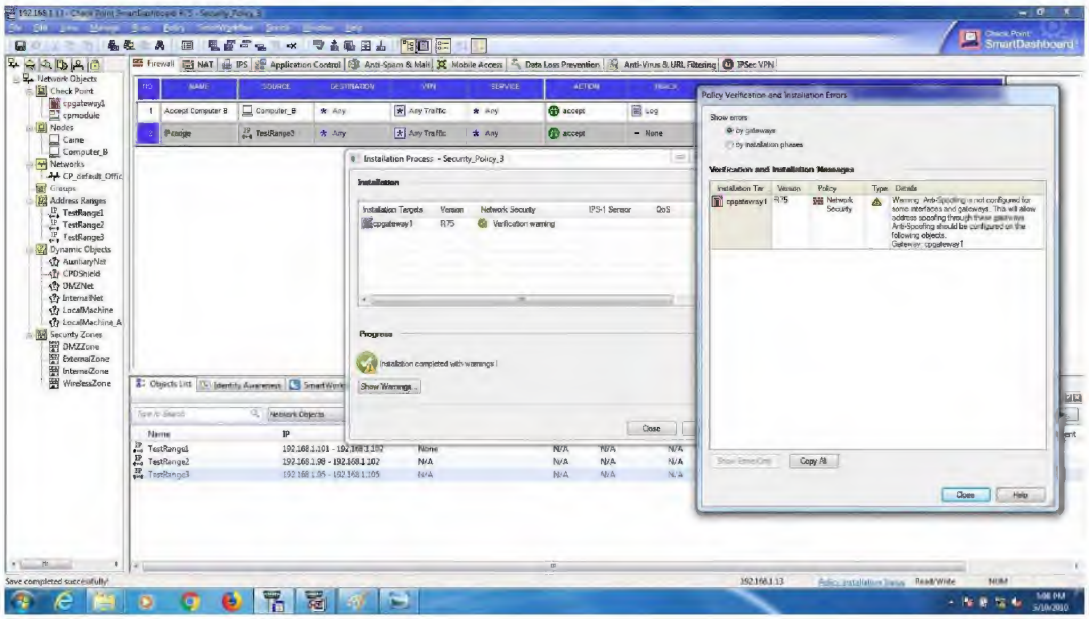


Figure 41. Screenshot of SmartDashboard GUI showing that a dynamic security policy specifying a third set of network addresses for which packets should be forwarded was received by Security Gateway 1 at 5:08 pm.

214. It has been demonstrated that Security Gateway 1 of the Check Point R75 system in Exponent's test setup received three dynamic security policies. The first policy forwarded

CENTRIPETAL-CSCO 087589

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 89

packets in the range 192.168.1.101 –192.168.1.102, the second policy forwarded packets in the range 192.168.1.98 – 192.168.1.102, and the third policy forwarded packets in the range 192.168.1.95 – 192.168.1.105. The first policy was received at 4:57 pm, the second policy was received at 5:04 pm, and the third policy was received at 5:08 pm.

215. Thus, we have demonstrated that the second policy was received after the first policy, and the third policy was received after the second policy. We have also demonstrated that the second set of network addresses included more network addresses than the first set, and the third set of network addresses included more network addresses than the second set

216. Hence, the Check Point R75 system has been shown to satisfy all requirements of claim element 17f of the '205 Patent.

217. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 17f of the '205 Patent.

218. **Claim 17g: receive packets associated with a network protected by the packet security gateway.** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

219. As was shown above in relation to claim element 17e, using tcpdump, SG 1 received packets associated with Network B, which is the network protected by SG 1. In particular, these packets were associated with Network B because their destination, Computer B, was within Network B. Consequently, it was demonstrated that the Check Point R75 system includes receiving packets associated with a network protected by the packet security gateway

220. Thus, the Check Point R75 system has been demonstrated to satisfy all requirements of element 17g of the '205 Patent.

221. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 17g of the '205 Patent.

222. **Claim 17h: and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

223. As detailed in relation to claim element 17a, the Check Point R75 system performs "packet transformation functions" that satisfy both parties' proposed construction for this term

224. As demonstrated in relation to claim elements 17c-h via ping requests, the Check Point R75 system performs these packet transformation functions "on a packet by packet basis," according to the "plurality of dynamic security policies" upon packets that are "associated with the network protected" by the Check Point R75 Security Gateway 1.

225. As detailed in relation to claim element 17a, the Check Point R75 system is able to perform packet transformation functions "other than forwarding or dropping the packets," as required by claim element 17h, at least because logging, monitoring, and rerouting constitute packet transformation functions that satisfy this requirement. By way of a more specific example, a demonstration of this logging functionality performed using the test setup described in relation to Figure 29 and Figure 30 is detailed below.

226. As shown in Figure 42, the Check Point R75 system has the ability to log information about network traffic.[61] For each rule in the rule base, matching events can be tracked. The gateways collect and send data to the security management server, which makes logs available for inspection via SmartView Tracker.

227. This logging process is a packet transformation function other than forwarding or dropping packets because it is a function applied to all packets that does not forward or drop packets. If a packet matches a rule from the rule base for which logging is activated, and the log does not already contain an event corresponding to that rule, and any other logging criteria are met, then some information from that packet will be logged.

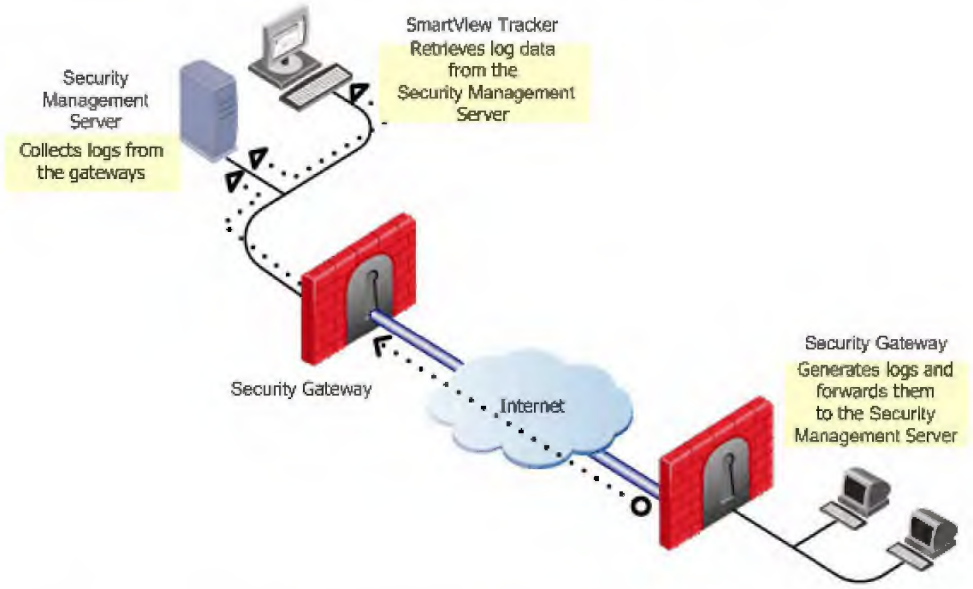


Figure 42. Illustration of possible configuration for logging packets from a security gateway.[62]

228. All three security policies that were installed on SG 1 tracked events corresponding to Rule 1 by logging (See red box in Figure 43 showing logging in the third security policy,

[61] See p. 65, "Check Point R75 Security Management Administration Guide" (dated Dec 15, 2010).
[62] See p. 65, "Check Point R75 Security Management Administration Guide" (dated Dec 15, 2010).

which was referenced in claim element 17f). Rule 1 allows traffic whose source is Computer B.

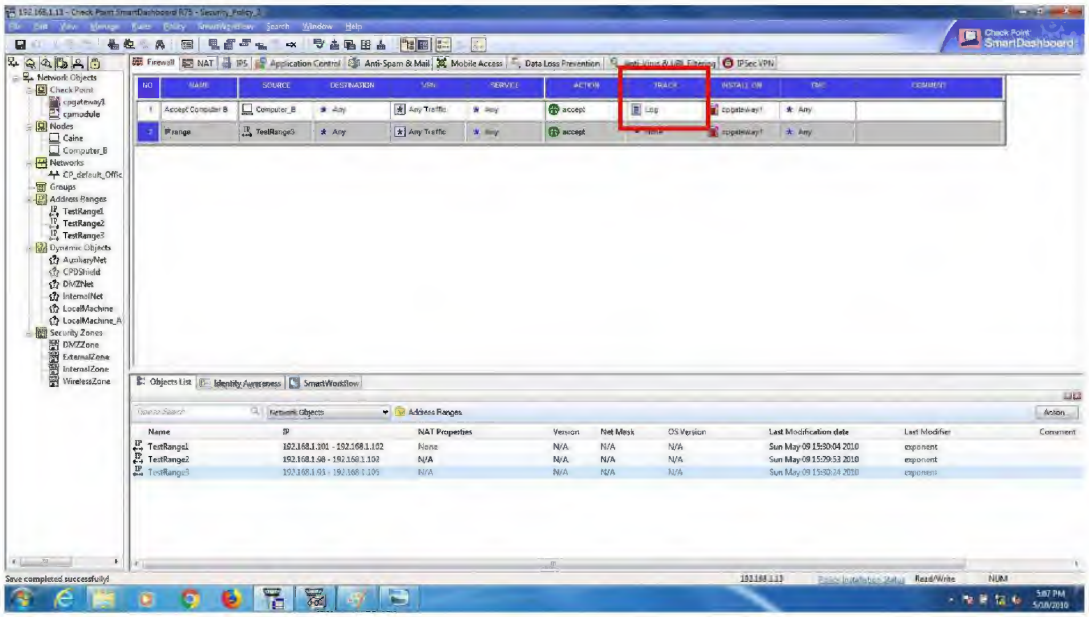


Figure 43. Saving a log file using the Check Point SmartView Tracker. The log contains data from 5:09 pm to 5:16 pm. During this time, the third dynamic security policy was installed on SG 1.

229. While the third security policy was installed on SG 1, logs were saved on the security management server and accessed using the SmartView Tracker on the GUI computer (see Figure 44).

CENTRIPETAL-CSCO 087593

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 93

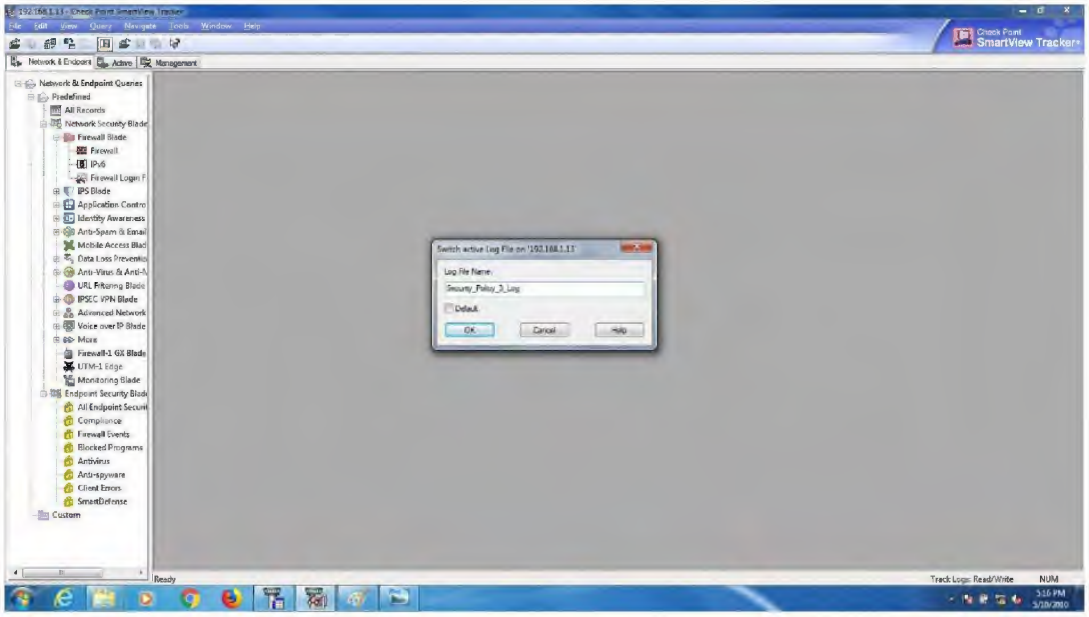


Figure 44. Saving a log file using the Check Point SmartView Tracker. The log contains data from 5:09 pm to 5:16 pm. During this time, the third dynamic security policy was installed on SG 1

230. While logging was occurring, "netcat" was used to open a connection between Computer A and Computer B. Listening on Computer A, an attempt was made to send a test packet of text ("test_packet") from Computer B on port 50001 (see Figure 45 and Figure 46). Another connection was opened on port 50002 and another test packet ("test_packet_2") was sent. Both packets were received by Computer A.

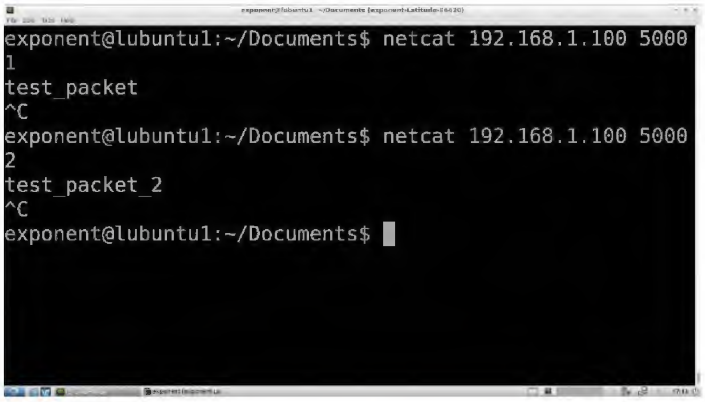


Figure 45. Sending packet of text ("test_packet") from Computer B ("lubuntu1") to Computer A (192.168.1.100) on port 50001 and then another packet ("test_packet_2") on port 50002.

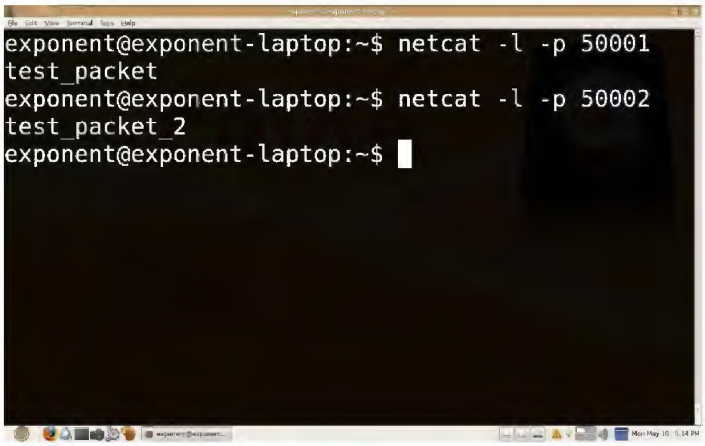


Figure 46. Listening for packets on port 50001 on Computer A ("exponent-laptop") and then on port 50002. One test packet was received on each port.

231. Using tcpdump to monitor traffic on interface eth0 of SG 1, SYN packets (highlighted in blue in Table 15) from Computer B were observed each time a connection was opened (at 17:13:04.4239 and at 17:13:33.3328). Data packets (highlighted in yellow in Table 15) from Computer B were also observed each time a packet of text was sent from Computer B to Computer A.

```
17:13:04.423911 172.16.1.99.45672 > 192.168.1.100.50001: S
3985798800:3985798800(0) win 29200 <mss 1460,sackOK,timestamp 2561690808
0,nop,wscale 7> (DF)
```


CENTRIPETAL-CSCO 087595

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 95

17:13:04.424489 192.168.1.100.50001 > 172.16.1.99.45672: S 1009837749:1009837749(0) ack 3985798801 win 5792 <mss 1460,sackOK,timestamp 64721913 2561690808,nop,wscale 7> (DF)
17:13:04.425094 172.16.1.99.45672 > 192.168.1.100.50001: . ack 1 win 229 <nop,nop,timestamp 2561690810 64721913> (DF)
17:13:11.474583 172.16.1.99.45672 > 192.168.1.100.50001: P 1:13(12) ack 1 win 229 <nop,nop,timestamp 2561697860 64721913> (DF)
17:13:11.474972 192.168.1.100.50001 > 172.16.1.99.45672: . ack 13 win 46 <nop,nop,timestamp 64723676 2561697860> (DF)
17:13:18.580028 172.16.1.99.45672 > 192.168.1.100.50001: F 13:13(0) ack 1 win 229 <nop,nop,timestamp 2561704966 64723676> (DF)
17:13:18.580638 192.168.1.100.50001 > 172.16.1.99.45672: F 1:1(0) ack 14 win 46 <nop,nop,timestamp 64725453 2561704966> (DF)
17:13:18.581088 172.16.1.99.45672 > 192.168.1.100.50001: . ack 2 win 229 <nop,nop,timestamp 2561704967 64725453> (DF)
17:13:33.332870 172.16.1.99.44628 > 192.168.1.100.50002: S 2710554287:2710554287(0) win 29200 <mss 1460,sackOK,timestamp 2561719719 0,nop,wscale 7> (DF)
17:13:33.333346 192.168.1.100.50002 > 172.16.1.99.44628: S 1478261631:1478261631(0) ack 2710554288 win 5792 <mss 1460,sackOK,timestamp 64729141 2561719719,nop,wscale 7> (DF)
17:13:33.333920 172.16.1.99.44628 > 192.168.1.100.50002: . ack 1 win 229 <nop,nop,timestamp 2561719721 64729141> (DF)
17:13:43.119155 172.16.1.99.44628 > 192.168.1.100.50002: P 1:15(14) ack 1 win 229 <nop,nop,timestamp 2561729506 64729141> (DF)
17:13:43.119668 192.168.1.100.50002 > 172.16.1.99.44628: . ack 15 win 46 <nop,nop,timestamp 64731588 2561729506> (DF)
17:14:10.850280 172.16.1.99.44628 > 192.168.1.100.50002: F 15:15(0) ack 1 win 229 <nop,nop,timestamp 2561757240 64731588> (DF)
17:14:10.850728 192.168.1.100.50002 > 172.16.1.99.44628: F 1:1(0) ack 16 win 46 <nop,nop,timestamp 64738521 2561757240> (DF)
17:14:10.851156 172.16.1.99.44628 > 192.168.1.100.50002: . ack 2 win 229 <nop,nop,timestamp 2561757241 64738521> (DF)

Table 15. Traffic between Computer A and Computer B as observed via the "tcpdump" utility on SG1.

232. The opening of these two connections was logged (see log file in Figure 47).

CENTRIPETAL-CSCO 087596

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 96

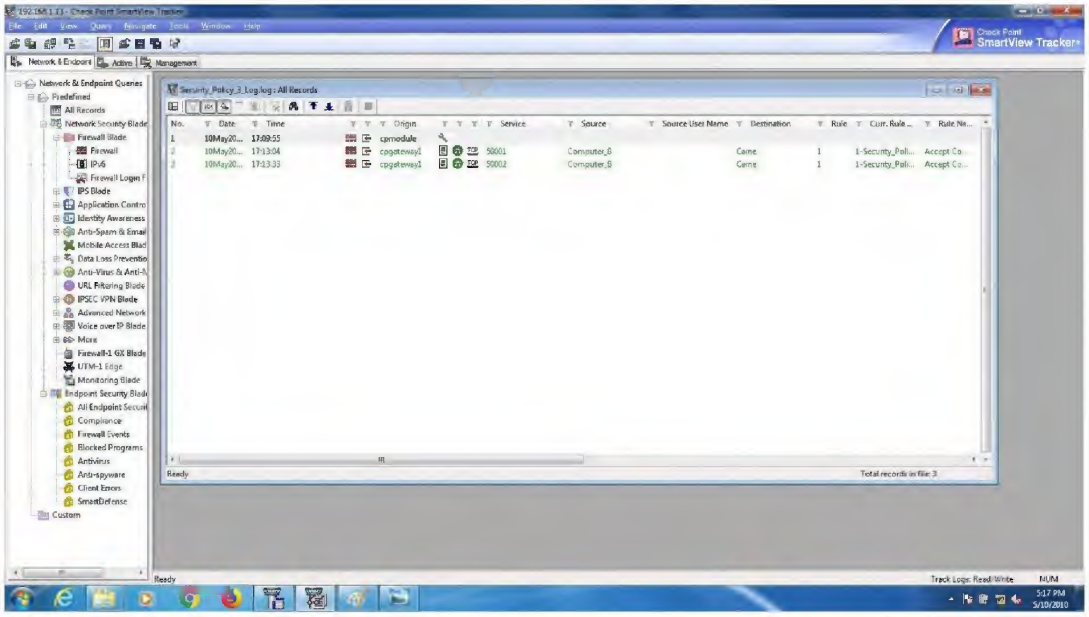


Figure 47. Log file containing data from 5:09 pm to 5:16 pm. During this time, the third dynamic security policy was installed on SG 1. Three events are recorded in the log. Event 1 records changing the name of the log file. Event 2 records opening the connection from Computer B on port 50001. Event 3 records opening the connection from Computer B on port 50002.

233. As shown in Figure 48, information from the packets was recorded in the log.

CENTRIPETAL-CSCO 087597

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 97

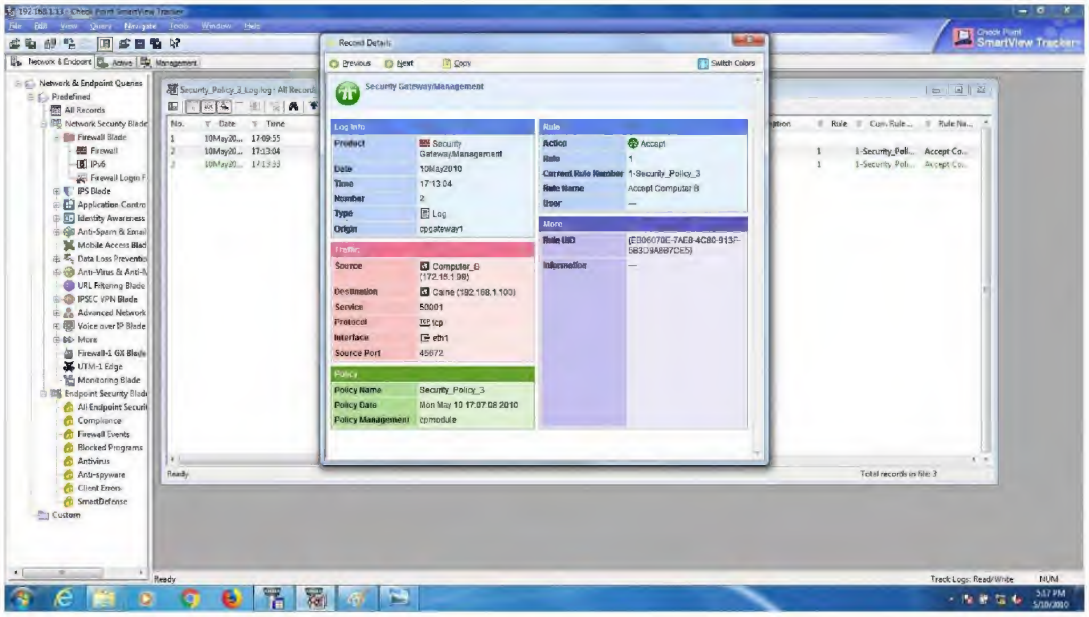


Figure 48. Information contained in record 2 of the log. Some information from the packet is present in the pink "Traffic" table, indicating that a packet transformation function other than forwarding or dropping was performed.

234. Thus, it has been demonstrated that the Check Point R75 system includes logging, and that logging is a packet transformation function other than forwarding or dropping that occurred in all three dynamic security policies installed on SG 1 on packets associated with Network B.

235. The Check Point R75 method also includes monitoring[63] (i.e. routing a packet to a monitoring device), which, similar to logging, is described in the '205 Patent as an example of a packet transformation function other than forwarding or dropping.[64]

236. The above testing demonstrates that the Check Point R75 system can apply "at least one packet transformation function other than forwarding or dropping the packets," at least because logging and monitoring constitute such packet transformation functions. Hence, the

63 See pp. 99 and 110 "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010). See also "Check Point R75 SmartView Monitor Administration Guide" (dated 17 April 2013).

64 '205 Patent, Column 7, Lines 27–36.

above demonstration, in conjunction with the testing described in relation to claim elements 17a-g, demonstrate that all requirements of claim element 17h are satisfied by the Check Point R75 system.

237. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 17h of the '205 Patent.

238. As detailed above, it is my opinion that all requirements of each and every element of Claim 17 of the '205 Patent are anticipated by the Check Point R75 system. Consequently, for at least the reasons above, it is my opinion that Claim 17 of the '205 Patent is anticipated by the Check Point R75 system

3. CLAIM 33

239. **Claim 33a: One or more non- transitory computer readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

240. For at least the reasons detailed in relation to claim 17 above, the Check Point R75 system comprises "packet security gateways" that are associated with a "security policy management server," where each of these terms is interpreted according to the relevant claim constructions.

241. Furthermore, the Check Point R75 installation comprises two Dell PowerEdge computers that contain hard drives and other computer memory, which constitute "non-transitory computer readable media"; and, these hard drive store programs and data resources required

to enable the Check Point R75 system to operate, which constitute "instructions stored thereon" for causing the packet security gateways to function.

242. Thus, for at least the reasons above, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33a of the '205 Patent.

243. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33a of the '205 Patent.

244. **Claim 33b: receive a plurality of dynamic security policies from the security policy management server.** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

245. As detailed in relation to claim element 17b above, the Check Point R75 SGs receive "a plurality of dynamic security policies" from the Check Point R75 SMS, which constitutes a "security policy management server," where said "dynamic security policies" satisfy the relevant claim constructions proposed by both parties.

246. Thus, for at least the reasons detailed in relation to claim 17, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33b of the '205 Patent.

247. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33b of the '205 Patent

248. **Claim 33c: receive at least one rule specifying a set of network addresses for which associated packets should be for warded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped.** It has been demonstrated that the Check Point R75 system satisfies all requirements of this claim element, as set forth in relation to claim element 17c above. Thus, for at least the same reasons as detailed in relation to claim

element 17c, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33c of the '205 Patent.

249. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33c of the '205 Patent

250. **Claim 33d: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded.** It has been demonstrated that the Check Point R75 system satisfies all requirements of this claim element, as set forth in relation to claim element 17d above. Thus, for at least the same reasons as detailed in relation to claim element 17d, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33d of the '205 Patent.

251. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33d of the '205 Patent.

252. **Claim 33e: receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded.** It has been demonstrated that the Check Point R75 system satisfies all requirements of this claim element, as set forth in relation to claim element 17e above. Thus, for at least the same reasons as detailed in relation to claim element 17e, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33e of the '205 Patent.

253. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33e of the '205 Patent

254. **Claim 33f: receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network**

addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses.. As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

255. It has been demonstrated that the Check Point R75 system satisfies all requirements of this claim element, as set forth in relation to claim element 17f above. Thus, for at least the same reasons as detailed in relation to claim element 17f, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33f of the '205 Patent.

256. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33f of the '205 Patent

257. **Claim 33g: receive packets associated with a network protected by the packet security gateway.** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

258. It has been demonstrated that the Check Point R75 system satisfies all requirements of this claim element, as set forth in relation to claim element 17g above. Thus, for at least the same reasons as detailed in relation to claim element 17g, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33g of the '205 Patent.

259. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33g of the '205 Patent

260. **Claim 33h: and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least**

one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets. As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

261. It has been demonstrated that the Check Point R75 system satisfies all requirements of this claim element, as set forth in relation to claim element 17h above. Thus, for at least the same reasons as detailed in relation to claim element 17h, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 33h of the '205 Patent.

262. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 33h of the '205 Patent.

E. OBVIOUSNESS IN VIEW OF US PATENT NO. 8,955,128 IN COMBINATION WITH POLIWALL AND NTO 5236

1. US PATENT NO. 8,955,128

263. US Patent No. 8,955,128 ("the '128 Patent"), entitled "Systems and Methods for Selectively Regulating Network Traffic," was filed on July 27, 2012.

264. The '128 Patent is directed towards "systems and methods for controlling traffic to a network. More particularly, the invention is directed to systems and methods for regulating network traffic based on user preferences" (the '128 Patent, 1:15-18). For example, "[n]etwork traffic from undesirable countries… can be blocked with the click of a mouse." ('128 Patent, Abstract).

265. The invention of the '128 Patent seeks to "provide a method for reducing unwanted network traffic via easily configured lists" (the '128 Patent, 2:55-57), where "lists" are files that contain IP addresses (*see* the '128 Patent, 4:8-14) that are used to identify packets to

which filtering rules should be applied. An objective of the '128 Patent is to allow filtering of packets based on, for example, country of origin, such that filters may be created to exclude all packets from pre-determined countries, or allow only packets from pre-determined countries. The invention of the '128 Patent contemplates the use of repositories that contain many lists, which may be updated from a "centralized server," stating:

> In an embodiment, the repository may be organized or compiled into any one or more of the following lists: Prebuilt Country IP lists, Subscribed Lists, Custom Lists, or Control Lists. The Prebuilt Contry IP Lists may be a pre-made list for each country. There files/lists may be updated from the centralized server 30 as information is obtained from the appliance 20. Subscribed Lists may include prebuilt lists which a user may choose to add or filter with. … Custom Lists are lists that the user can create based on their own criteria … Other lists which are not based on geographical boundaries may also be utilized. (the '128 Patent, 4:18-35)

266. In another example embodiment, the '128 Patent describes that non-geographical-based filtering is also considered therein, disclosing "common filtering methods based on websites such as gambling, pornographic, narcotics, and the like" (the '128 Patent, 10:12-13).

267. Packets are filtered by a "rules engine" which uses "predefined rules to evaluate incoming information based on one or more predefined rules … determined by a user's preferences" (the '128 Patent, 3:42-46), and "[t]he desired lists … may be selected or turned on by the user through the user interface" (the '128 Patent, 4:36-37).

268. The '128 Patent discloses that the filtering device may be "located at any number of locations so long as it sits in between the Internet and the network it is designed to protect" (the '128 Patent, 4:43-45). The appliance may also be a network transparent "Layer 2 network bridge" (the '128 Patent, 4:45-48). The use of packet-by-packet application of filtering rules upon packets that match criteria is also disclosed:

> In operation, when network traffic, such as individual packets, attempt to enter a network protected by the system of the invention, rules are applied, they are loaded into the network filter of the system in various chains as appreciated by one skilled in the art. As used herein, a "chain" refers to a series of rules that are applied to the incoming packets such that they can be handled in a pre-defined and automated way depending on whether or not they satisfy certain criteria or have certain characteristics (the '128 Patent, 4:49-57, emphasis added).

269. The invention of the '128 Patent may perform one or more actions to packets which satisfy the criteria of one or more rules. These actions can include: forwarding packets to the intended destination (*see* the '128 Patent, e.g. 4:61-67); dropping packets (*see* the '128 Patent, e.g. 5:1-24); logging packets (*see* the '128 Patent, e.g. 6:37-40).

270. The system disclosed by the '128 Patent also features a graphical user interface, which in addition to enabling the user to customize and select lists, and associated rules, also "display[s] real-time statistics" relating to network traffic, and enables the user to access various logs, alerts, and notifications (*see* the '128 Patent, e.g. 8:36-48; *see* the '128 Patent, Fig. 3).

2. POLIWALL

271. According to the testimony of the Chief Technology Officer responsible for the TechGuard PoliWall packet filtering device ("PoliWall"), PoliWall has been available since at least 2006.[65] Other documentation supports his testimony, including as follows:

a. On September, 29, 2009 Techguard issued a press release for the PoliWall-ESE line of security appliances. See WayBack Machine Nov 27 2009 capture of TechGuard Website

[65] July 26, 2018 Deposition Transcript of David Masteas, CTO of Bandura, a wholly-owned subsidiary of TechGuard. .

CENTRIPETAL-CSCO 087605

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 105

(https://web.archive.org/web/20091127221108/http:/techguard.com:80/docs/TGS_Poliwall_ESE_092909.pdf).

b. Also on September 29, 2009, media outlet TMC Net.Com published an article titled "TechGuard Unveils PoliWall ESE Line of Security Appliances for Data Center, Enterprise, SMB and SOHO". Sept 29 2009 TMCNet.com Article (https://www.tmcnet.com/usubmit/2009/09/29/4395554.htm).

c. An October 13, 2009 interview with TechGuard CEO Suzanne Magee published on ZDNet confirms the availability of PoliWall ESE in 2009. Oct. 13, 2009 ZDNet Article (http://www.zdnet.com/article/techguard-keeps-spam-and-botnets-at-bay-with-one-click-enterprise-level-security-for-smbs-sohos/).

d. TechGuard's Invoice Spreadsheet of PoliWall sales indicates a sale of PoliWall Modell PW-ESE-M50-01C on December 31, 2009.BAND-TGS00469.

e. The User's Manual for PoliWall-ESE Version 2.00.01 indicates that "This edition published September 2010. © 2010 TechGuard Security, L.L.C." and has a hand-written date of September 9, 2010. BAND-TGS00250.

f. On January 26, 2011, Booz Allen Hamilton Common Criteria Testing Laboratory issued a review of PoliWall-CCF v. 2.01.01. (st_vid10346-st.pdf).

g. On March 23, 2011, the National Information Assurance Partnership released the Common Criteria Evaluation and Validation Scheme Validation Report for TechGuard Security PoliWall-CCF v. 2.01.01. (st_vid10346-vr.pdf).

h. On May 17, 2011, EDN Network published an article discussing PoliWall products that had achieved Common Criteria EAL 4+ validation. May 17 2011 EDN Network TechGuard PoliWall Joins the Ranks of the Elite Few to Achieve

Common Criteria EAL 4+ Validation (https://www.edn.com/Home/PrintView?contentItemId=4219800).

i. Centripetal's emails memorialize that Poliwall was "in production by early-mid 2011 at the latest." CENTRIPETAL0060981.

272. PoliWall was advertised as "a high performance security appliance to thwart global network threats and analyze cyber attacks." This is achieved by placing PoliWall between a router (which may be connected to the Internet) and a network firewall, as depicted below in section of the PoliWall brochure.

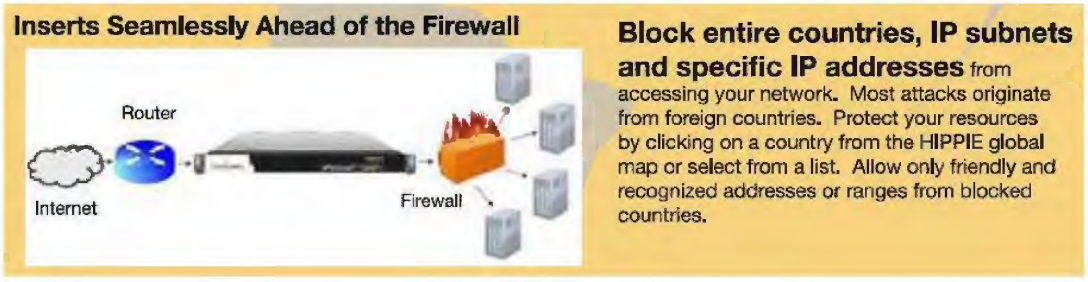


Figure 49 Excerpt from PoliWall brochure

273. PoliWall used its High-speed Internet Protocol Packet Inspection Engine ("HIPPIE") to enable rules to be applied to packets based upon their IP address of origin. This enabled users to set rules based upon geographical locations such that traffic from particular countries may be restricted. In addition to allowing all traffic from a particular country to be blocked, PoliWall also enabled a user to configure rules to enable all traffic from particular countries to be trusted and thus forwarded without restriction. Examples of restricting and allowing all traffic from particular countries is shown in a YouTube video[66] published on March 3, 2011, which counsel informs me constitutes a prior art reference under applicable law.

[66] https://www.youtube.com/watch?v=z62og8lNk5A

3. NTO 5236

274. The Anue Network Tool Optimizer™ NTO 5236 ("NTO 5236") is a network packet broker system for aggregating, filtering, and directing network data to tools such as data recorders, VoIP monitors, or other applications. This system comprises a device with network ports and tool ports. A typical usage case for the system is in a large network where traffic must be routed to many individual tools. The NTO 5236 can filter packets to reduce the load on the tools and balance the packet load among groups of tools.

275. The NTO 5236 system was commercially available to purchase prior to the priority date of the '205 Patent.[67] The functionality of the NTO 5236 is documented in the NTO 5200 User Guide.[68]

276. The NTO 5236 assists in network optimization by enabling network traffic to be filtered and directed to the appropriate device. For example, "[t]he Anue Net Tool Optimizer (NTO) directs network data from SPAN ports and TAPS in your data center and forwards it to a convenient centralized tool farm where multiple tools can share simultaneous access to the network data" (PA0000777); and "[i]nbound traffic from any incoming port may be switched to one or more outgoing ports … Ports designated through software are Tool Ports are used to connect tools such as data recorders and VoIP monitors … the Control Panel client, a Java based graphical user interface (GUI), is proved so that the configuration and visualization of part mappings is easy and intuitive" (PA0000777). This tool optimization is depicted in Figure 1-1 on PA0000777, which is reproduced herein.

[67] See Declaration of Dario David dated May 25, 2018.
[68] Starting at PA0000777

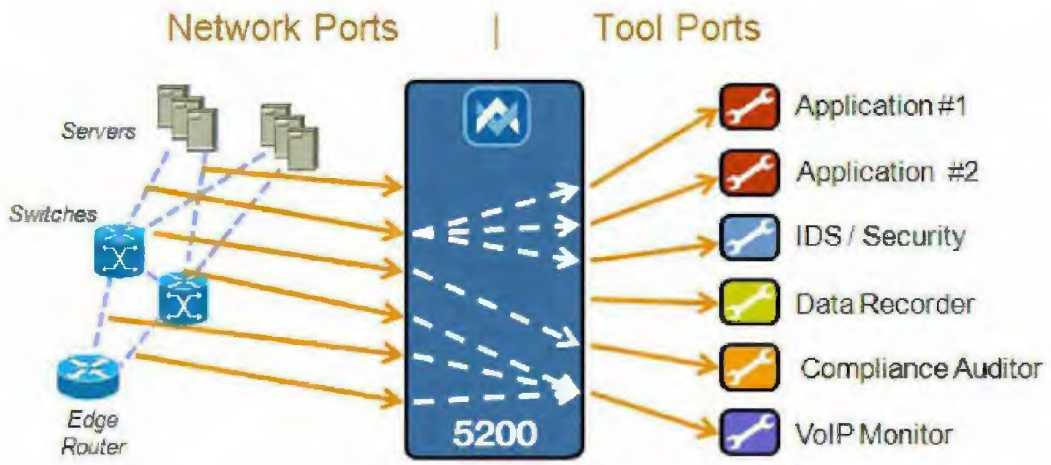


Figure 1-1. Anue NTO Tool Optimization

Figure 50 Reproduced from NTO 5200 manual (PA0000777).

277. The NTO 5236 enables various filter types to be applied, as described in PA0000780-82, which apply user-configurable rules to packets which match associated filter criteria. Packets which match applicable rules are subjected to a range of potential actions, including being allowed or denied to continue towards their destination, and/or logging.

278. The NTO filtering is configurable via a GUI, a screenshot from the Control Panel of which is provided below (reproduced from PA0000813).

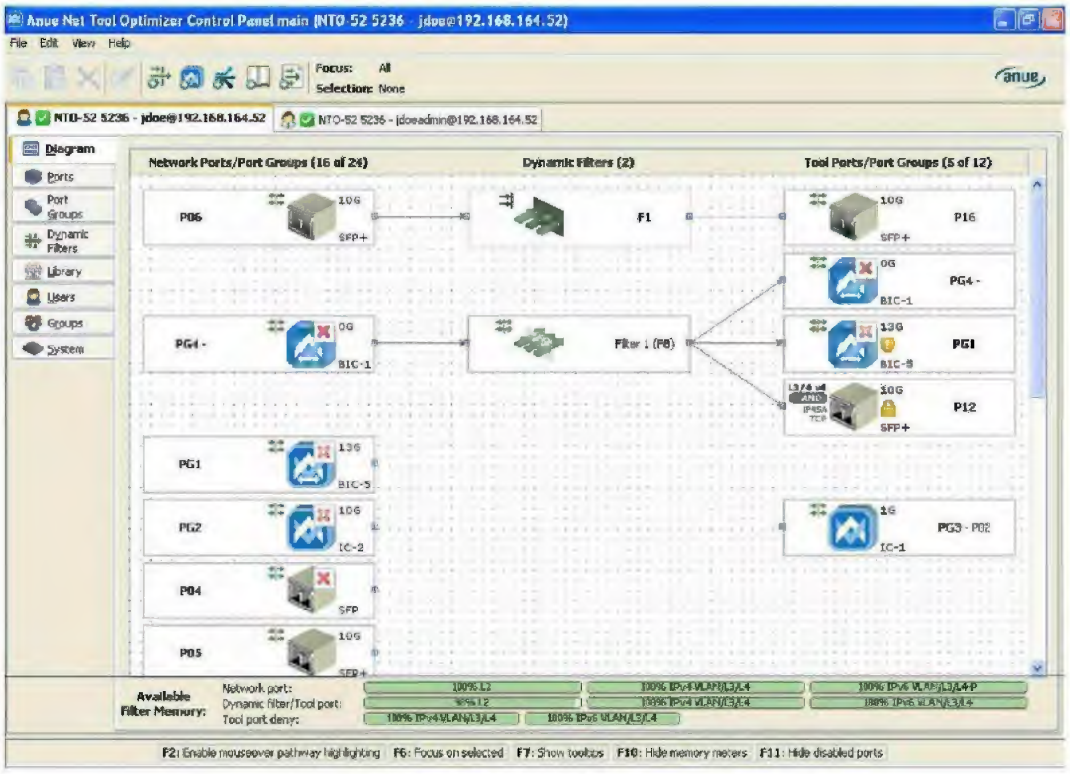


Figure 4-11. Control Panel

Figure 51 Screenshot showing the Control Panel overview of an NTO 5200 Series GUI (reproduced from PA0000813).

4. NTO 5200 User Guide

I was provided with the user guide for the NTO 5236, dated October 2013, as shown in

ixia

Anue Net Tool Optimizer 5200 Series
User Guide

NVOS 3.9, October 2013

279. Figure 197. I am informed by counsel that previous user guides are similar to this one.



Anue Net Tool Optimizer 5200 Series
User Guide

NVOS 3.9, October 2013

Figure 52. The title page of the NTO 5236 User Guide, dated October 2013.

280. I analyzed this user guide to evaluate whether the NTO 5236 system enables a person of ordinary skill in the art to practice the claim elements of the '205 Patent

5. MOTIVATION TO COMBINE

281. The network filtering appliance of the '128 Patent, PoliWall product, and NTO 5236, are all directed towards the same field of endeavor: enhancing network security and traffic optimization. Each of these prior art systemss addresses this field in a similar manner, by applying filtering to traffic on a packet-by-packet bases to enforce a policy comprised of various rules, where each rule is applicable only to packets that match certain criteria or conditions.

282. More specifically, the network filtering appliance of the '128 Patent and PoliWall both include functionality that enables filtering of packets based on their geographical origin. The '128 Patent includes example embodiments where traffic is restricted from particular countries using a centralized server that updates lists of IP addresses associated with a given region; and also examples of using other data that is non-geographical for filtering purposes.

PoliWall includes an intuitive GUI that enables a user to conveniently select IP addresses from countries and apply various rules including drop, trust (forward), or log. A POSITA would recognize that a combination of the GUI elements of PoliWall with the centralized server update mechanism, and additional non-geographical filtering criteria, of the '128 Patent would result in an improved system that overcomes shortcomings of each individual prior art. For example, the automatic updating of IP addresses using information from the Internet Name and Number regulatory authorities (*see* e.g. the '128 Patent, 3:54-63) would enable PoliWall to rapidly adapt to newly issued IP addresses, and would improve the accuracy of rules based upon country selections made via the PoliWall GUI.

283. The NTO 5236 is directed towards optimization of traffic over a large network that includes a range of different tools/functionalities. Thus, the NTO 5236 acts as a packet broker that can filter packets to reduce the load on the tools and balance the packet load among groups of tools. For example, a network may include multiple instances of a service to increase capacity and the NTO 5236 can identify packets addressed to said service and distribute them between the multiple instances to optimize the loading and thereby increase performance of said service. Alternately, a network may have several different services that each handle a different kind of traffic, and the NTO 5236 can direct appropriate packets to their corresponding service. This enables specialized tools to process relevant packets and thus increase the overall performance of a network. A POSITA would recognize that the packet brokering of the NTO 5236 can be combined with the security filtering of the PoliWall, the filtering appliance of the '128 Patent, or a combination of the two. Furthermore, a POSITA would understand that such a combination would enable the security filtering provided by security gateways to first protect a network from threats, before the

allowed traffic is subsequently optimized throughout the protected network by the NTO 5236.

284. Thus, a POSITA would recognize that a combination of the centralized server update mechanism, and non-geographical filter criteria, of the '128 Patent with the packet filtering and rule-creation GUI of the PoliWall, and network traffic optimization of the NTO 5236 packet broker functionality, would result in a system that confers benefits over and above those offered by each prior art in insolation. At least due to the mutual use of IP packets, which by their nature are designed to be compatible across numerous devices, and because this combination can be made without significant modifications to any prior art, a POSITA would understand that such a combination would be likely to succeed without undue experimentation.

285. Therefore, for at least the reasons above, it is my opinion that a POSITA would have been motivated to combine the packet filtering of the PoliWall, enhanced with the centralized server update functionality of the '128 Patent, with the network traffic optimization of the NTO 5236 packet brokering functionality.

286. As detailed below, it is my opinion that the prior art combination identified above renders obvious claims 17 and 33 of the '205 Patent.

6. CLAIM 17

287. **Claim 17a: A system, comprising: security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to.** The '205 Patent states that "[a]s used herein, a security policy management

CENTRIPETAL-CSCO 087613

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 113

server includes any computing device configured to communicate a dynamic security policy to a packet security gateway."[69] I understand, however, that the parties have agreed that the term "security policy management server" is to be construed as "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway,"[70] and I have applied this claim construction throughout my analysis. The combination described above comprises a security policy management server, for at least the following reasons.

288. The '128 Patent discloses a "Central Server" that is used to communicate dynamic security policies to a packet filtering appliance, describing in an example embodiment that the lists which contain filtering information may be "updated from the centralized server 30" (the '128 Patent, 4:23-24), and stating, in relation to the configuration of the filtering appliance, "the hardware appliance may be updated periodically, such as daily, monthly, or annually from server 30" (the '128 Patent, 3:32-34). More specifically, the '128 Patent discloses that

> In an embodiment, a centralized server may include a repository or database for updates and content information for the appliance and/or user. For example, the centralized server may store lists of IP addresses by region, store additional details about the IP addresses, such as host name, location information and the like … The repositories on the server may be updated daily or as frequently as desired by querying the Internet Name and Number regulatory authorities (the '128 Patent, 3:54-63).

289. Therefore, the '128 Patent discloses "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway" as required by the claim construction of "security policy management server."

---

[69] '205 Patent, at 4:37-40.
[70] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.

290. The '205 Patent states that "[a]s used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation on the packets."[71] I understand, however, that the parties have agreed that the term "packet security gateway" is to be construed as "a gateway computer configured to receive packets and perform a packet transformation function on the packets,"[72] and I have applied this claim construction throughout my analysis.

291. I also understand that there is a dispute regarding the construction of the term "packet transformation function." More specifically, Plaintiffs have proposed that this term be construed as "function that transforms packets from one state to another" while Defendants have proposed "an operation performed on a packet specified by the dynamic security policy, such as forward or drop."[73] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination described above comprises "one or more packet security gateways," as detailed below.

292. The '128 Patent discloses a network filtering appliance, which "may be a hardware appliance or may be a virtual appliance," where "[a] hardware appliance includes a physical box, such as typical server hardware from Dell, HP, IBM, and other hardware providers" ('128 Patent, 3:23-26). Thus, the filtering appliance of the '128 Patent comprises standard computing hardware, and is configured to filter packets, which requires the ability to both receive packets and perform packet transformations upon the packets. Therefore, the '128 Patent discloses a "packet security gateway."

---

[71] '205 Patent, at 4:33-35.
[72] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.
[73] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

CENTRIPETAL-CSCO 087615

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 115

293. Similarly, the PoliWall filtering device comprises a standard rack mountable chassis, and well-known computing hardware including: a Intel Xeon 3070 processor, several GB of RAM, internal storage via a HDD, and various Ethernet ports. The PoliWall device is intended to be located at the interface between the Internet and the network that it protects, and functions by receiving packets from an Internet-connected router and determining whether to forward these packets to the protected network. Thus, PoliWall also includes a "packet security gateway" as required by this claim element.

294. Also, the NTO 5236 includes standard hardware for receiving packets and routing them appropriately.

295. As described above, there is a dispute as to the interpretation of "packet transformation function," however, the '128 Patent and PoliWall each satisfy both proposed constructions for this term. Plaintiff's proposed construction of "packet transformation function" requires a function that "transforms one or more packets from one state to another." Although Plaintiff's have not provided an explicit definition for transforming "from one state to another," the intrinsic evidence cited to by Plaintiff in support of their proposed construction includes example embodiments in which packets are forwarded or dropped depending upon parameters of the packet such as the origination IP address. Thus, under Plaintiff's proposed construction, forwarding or dropping of packets constitutes transforming a packet from one state to another, and hence forwarding or dropping satisfy Plaintiff's construction of "packet transformation function." Similarly, Defendants' proposed construction for "packet transformation function" explicitly includes the operations "forward or drop," and hence forwarding or dropping also satisfy Defendant's proposed construction for this term. Thus, at least because the filtering appliance of the '128 Patent and the PoliWall can each either

forward or drop packets, these prior arts satisfy either proposed construction for "packet transformation function."

296. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 17a of the '205 Patent, and thus renders this claim element obvious.

297. **Claim 17b: receive a plurality of dynamic security policies from the security policy management server.** I understand there is a dispute regarding the construction of the term "dynamic security policy." More specifically, Plaintiff has proposed that this term be construed as "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets," while Defendants have proposed that this term be construed as "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria".[74] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination identified above satisfies all requirements of this claim element, for at least the reasons detailed below.

298. As detailed above in relation to claim element 17a, the '128 Patent discloses a packet security gateway disclosed therein (i.e. the network filtering appliance) that communicates with a "security policy management server" (i.e. the centralized server), as required by this claim element and the associated claim construction agreed upon by both parties.

299. The '128 Patent discloses a "rules engine" which is used "to evaluate incoming information based on one or more predefined rules" (the '128 Patent, 3:41-44). These rules

[74] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

are also disclosed to be applied on a packet-by-packet basis to network traffic, and "are applied to incoming packets such that they can be handled in a pre-defined and automated way depending on whether or not they satisfy certain criteria of have certain characteristics" (*see* e.g. the '128 Patent, 4:49-60). The rules can be set to handle packets that match specific criteria by either dropping or accepting the packet (*see* e.g. the '128 Patent, 5:1-47). In addition to dropping and accepting, the '128 Patent also discloses logging (*see* e.g. the '128 Patent, 8:50-10:7). The rules comprise "lists" or "files" (where these terms are explicitly used interchangeably) which thus satisfies both proposed constructions for "dynamic security policy."

300. As detailed above in relation to claim element 17a, the '128 Patent discloses updating rules from a centralized server, thus satisfying the requirements of claim element 17b that the security gateway "receive a plurality of dynamic security policies from the security policy management server."

301. For at least the reasons above, it is my opinion that the '128 Patent discloses the requirements of this claim element. Consequently, it is my opinion that the prior art combination identified above renders claim element 17b of the '205 Patent obvious.

302. **Claim 17c: receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped.** I understand there is a dispute regarding the construction of the term "rule." More specifically, Plaintiff has proposed that this term be construed as "condition or set of conditions that when satisfied cause a specific action to occur," while Defendants have proposed that this term be construed as "(i) packet-identifying

criteria and (ii) a function to be performed on the identified packets."[75] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination identified above satisfies all requirements of this claim element, for at least the reasons detailed below.

303. The '128 Patent, PoliWall, and NTO 5236 each use "rules" which satisfy both proposed constructions for this term. For example, the '128 Patent discloses a "rules engine" which either drops, forwards, or logs, packets that match criteria, or conditions, set forth in various "lists." PoliWall enables the creation of rules based on the origin IP address of packets, these rules can be set to drop, forward, or restrict (i.e. throttle) traffic from user-selected countries; thus, packets that match certain criteria, or conditions, relating to origination IP address are subjected to a packet transformation function. The PoliWall YouTube video presents an example of creating a security policy that contains a list of IP addresses from North America that are allowed to be forwarded or blocked, thus satisfying this claim element.[76] NTO 5236 routes packets using rules that are based on criteria of the packets, such that packet which match criteria, or conditions, for a given rule are routed according to said rule.

304. Thus, a POSITA would have understood that the prior art combination discussed above could be used to receive at least one rule specifying a set of network addresses for which associated packets should be forwarded, and at least one rule specifying that packets associated with network addresses out of said set should be dropped.

---

[75] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

[76] Examples of rule creation, and explanation of these rules, is provided in the PoliWall YouTube video at https://www.youtube.com/watch?v=z62og8lNk5A

305. For at least the reasons above, it is my opinion that the '128 Patent alone or in combination with PoliWall and/or NTO 5236 discloses the requirements of this claim element. Consequently, it is my opinion that the prior art combination identified above renders claim element 17c of the '205 Patent obvious.

306. **Claim 17d: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded.** The '128 Patent, PoliWall, and NTO 5236 each use "rules" which comprise a dynamic security policy, in accord with the corresponding claim constructions discussed above. The '128 Patent discloses a "rules engine" which either drops, forwards, or logs, packets that match criteria, or conditions, set forth in various "lists," including "trusted lists" which comprise IP addresses for which packets should be forwarded as required by this claim element. PoliWall enables the creation of rules based on the origin IP address of packets, these rules can be set to drop, forward, or restrict (i.e. throttle) traffic from user-selected countries; thus, packets that match certain criteria, or conditions, relating to origination IP address are subjected to a packet transformation function. The PoliWall YouTube video presents an example of creating a security policy that contains a list of IP addresses from North America that are allowed to be forwarded, thus satisfying this claim element.[77] NTO 5236 routes packets using rules that are based on criteria of the packets, such that packet which match criteria, or conditions, for a given rule are routed according to said rule.

307. The example embodiments of the '128 Patent include the filtering appliance therein receiving list of rules from a centralized server, and thus the '128 Patent discloses the limitations of claim element 17d.

[77] Examples of rule creation, and explanation of these rules, is provided in the PoliWall YouTube video at https://www.youtube.com/watch?v=z62og8lNk5A

308. The typical usage cases for PoliWall and NTO 5236 involve configuring their respective security gateways with rules that can be modified by users, or in response to network-threats. Therefore, a POSITA would recognize that in order to function as intended, the PoliWall and NTO 5236 satisfy all requirements of claim element 17d. Indeed, an example of dynamic security policies being configured is included in the PoliWall YouTube video.[77]

309. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 17d, and thus renders this claim element obvious.

310. **Claim 17e: receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded.** For at least the same reasons as detailed above in relation to claim element 17d, the prior art combination identified above satisfies all requirements of claim element 17e. More specifically, a POSITA would understand that receiving sets of filtering rules to specify network addresses for which packets should be forwarded is required in order for the invention of the '128 Patent, PoliWall, and NTO 5236 to operate as intended.

311. Consequently, a POSITA would recognize that each packet filtering device, and their associated security gateways, within the prior art combination identified above must necessarily satisfy the requirements of claim element 17e. Therefore, it is my opinion that claim element 17e is obvious in view of the prior art combination described above.

312. **Claim 17f: receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses,**

CENTRIPETAL-CSCO 087621

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 121

and the third set of network addresses including more network addresses than the second set of network addresses. For at least the same reasons as detailed above in relation to claim element 17d, the prior art combination identified above satisfies all requirements of claim element 17e. More specifically, a POSITA would understand that receiving sets of filtering rules to specify network addresses for which packets should be forwarded is required in order for the invention of the '128 Patent, PoliWall, and NTO 5236 to operate as intended.

313. Consequently, a POSITA would recognize that each packet filtering device, and their associated security gateways, within the prior art combination identified above must necessarily satisfy the requirements of claim element 17e. Although the prior art combination identified above does not explicitly provide an example of three particular sets of network addresses for which packets should be forward, where each subsequent set includes more IP addresses than the previous set, a POSITA would be readily able to implement this configuration if desired. Indeed, the ordinary course of duty of a POSITA responsible for security network traffic is likely to involve updating various "white lists" (which constitute sets of IP addresses for which packets are forwarded) to reflect any changes to network activity or trusted partner locations. In addition, I note that the '205 Patent does not disclose any particular advantage, benefit, or the like, associated with the specific claimed sequence of three progressively larger sets of IP addresses for which packets are forwarded.

314. In any event, based on the marketing material for PoliWall, which discloses the risks of opening a network to foreign traffic and also the benefits of restricting traffic to a local area close to a place of business, a typical use of the PoliWall system would be to restrict traffic such that only traffic from increasingly large geographical areas around a business are

included. Therefore, this typical usage case for PoliWall is likely to often result in exactly the sequence of security policies required by claim element 17f of the '205 Patent.

315. Therefore, for at least the reasons above, it is my opinion that claim element 17f is obvious in view of the prior art combination described above.

316. **Claim 17g: receive packets associated with a network protected by the packet security gateway.** Each of the prior arts within the combination identified above comprises at least one security gateway that receives packets associated with a network protected by said gateway during the normal course of typical use. Indeed, in order to function, the prior arts within the combination identified above necessarily must receive packets.

317. Therefore, for at least the reasons above, it is my opinion that claim element 17g is obvious in view of the prior art combination described above.

318. **Claim 17h: and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.** The prior art combination identified above must necessarily satisfy this claim element in order to function. Therefore, it is my opinion that said combination renders this claim element obvious.

319. For at least the reasons detailed above, it is my opinion that the prior art combination described above renders obvious each and every claim element of Claim 17 of the '205

Patent. Consequently, it is my opinion that Claim 17 of the '205 Patent is rendered obvious in view of the prior art combination described above.

7. CLAIM 33

320. **Claim 33a: One or more non- transitory computer readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:** For at least the reasons detailed in relation to Claim 17 above, the prior art combination identified above comprises "packet security gateways" that are associated with a "security policy management server," where each of these terms is interpreted according to the relevant claim constructions.

321. Furthermore, each of the prior arts in the combination identified above contain storage, such as HDD storage, which stores programs and data resources required to enable the device to function. A POSITA would recognize that the internal storage of the filtering hardware within the prior art combination described above is used to store information that includes instructions for controlling the respective device's pack security gateway.

322. Therefore, for at least the reasons above, it is my opinion that claim element 33a is obvious in view of the prior art combination identified above.

323. **Claim 33b: receive a plurality of dynamic security policies from the security policy management server.** As detailed in relation to claim element 17b, the prior art reference combination identified above satisfies all requirements of this claim element.

324. Therefore, for at least the reasons above, it is my opinion that claim element 33b is obvious in view of the prior art combination identified above.

325. **Claim 33c: receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped.** As detailed in relation to claim element 17c, the prior art reference combination identified above satisfies all requirements of this claim element.

326. Therefore, for at least the reasons above, it is my opinion that claim element 33c is obvious in view of the prior art combination identified above.

327. **Claim 33d: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded.** As detailed in relation to claim element 17d, the prior art reference combination identified above satisfies all requirements of this claim element.

328. Therefore, for at least the reasons above, it is my opinion that claim element 33d is obvious in view of the prior art combination identified above.

329. **Claim 33e: receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded.** As detailed in relation to claim element 17e, the prior art reference combination identified above satisfies all requirements of this claim element.

330. Therefore, for at least the reasons above, it is my opinion that claim element 33e is obvious in view of the prior art combination identified above.

331. **Claim 33f: receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network**

addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses. As detailed in relation to claim element 17f, the prior art reference combination identified above satisfies all requirements of this claim element.

332. Therefore, for at least the reasons above, it is my opinion that claim element 33f is obvious in view of the prior art combination identified above.

333. **Claim 33g: receive packets associated with a network protected by the packet security gateway.** As detailed in relation to claim element 17g, the prior art reference combination identified above satisfies all requirements of this claim element.

334. Therefore, for at least the reasons above, it is my opinion that claim element 33g is obvious in view of the prior art combination identified above.

335. **Claim 33h: and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets**. As detailed in relation to claim element 17h, the prior art reference combination identified above satisfies all requirements of this claim element.

336. Therefore, for at least the reasons above, it is my opinion that claim element 33h is obvious in view of the prior art combination identified above.

XI. U.S. PATENT NO. 9,264,370

337. I have been asked to review the '370 Patent and assess whether the limitations of claim 61 (which includes the limitations of claim 43 from which it depends) recite generic computer components or well-known, routine, or conventional activities.

338. It is my opinion that the components recited in claim 61 were generic and conventional before the '370 patent's filing date. The '370 patent discloses that the claimed functionality is not limited to any specific computing device, and may instead be implemented on one or more generic and well-known computing devices:

> The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer-executable instructions and computer-usable data described herein.
>
> Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, system, apparatus, or one or more computer-readable media storing computer-executable instructions. Accordingly, aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.
>
> As described herein, the various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like).

('370 Patent, 14:9-44.)

339. Further, generic devices that could be placed in communication links, network devices, host computers, and a computer system as recited in claims 43 and 61 were well-known in the industry before the filing date of the '370 patent.

XII. U.S. PATENT NO. 9,413,722

340. I have been asked to review the '722 Patent and assess the validity of claims 1 and 25 therein in view of the prior art referenced below. I will first summarize the '722 patent briefly and then discuss a claim-by-claim invalidity analysis.

A. SUMMARY OF THE '722 PATENT

341. The '722 patent assigned to Centripetal Networks, Inc., Herndon, VA (US), was filed on Sep. 15, 2015 and published on Aug. 9, 2016. The '722 patent relates to a rule-based network threat detection by a packet-filtering device. Specifically, it relates to the process of generating informative logs, where in the logs include information from the invoked packet-filtering rule that identifies network-threat indicator(s). The log also identifies if the packet was blocked or allowed to continue to its destination.[78]

342. Figure 53 illustrates an exemplar environment for rule-based network-threat detection including three networks A, B, and C, comprising of various hosts and protected by three packet filtering devices. Network D is a fourth network that interfaces networks A-C with each other, other networks, rule providers, network-threat-intelligence providers, threat hosts, and benign hosts.[79] Network-threat-intelligence providers communicate to rule providers regarding one or more network threats including one or more associated network threat indicators, e.g., network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs) and

[78] '722 patent, at 1:45-63.
[79] '722 patent, at 2:59-3:18.

uniform resource identifiers (URIs).[80] Based on this information, rule provider generates packet-filtering rules and communicates the rules to packet filtering devices.[81]

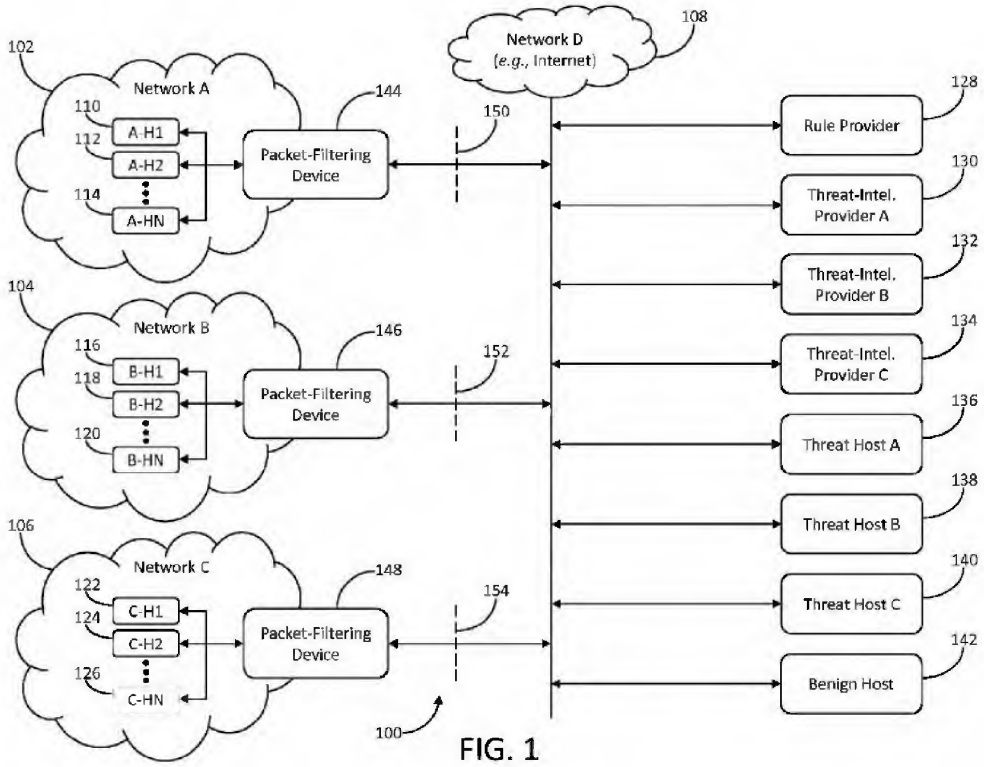


FIG. 1

Figure 53. An illustrative environment for rule-based network-threat detection ('722 Patent, FIG.1).

343. Figure 54 illustrates a flow diagram for rule-based network-threat detection. Packet filtering devices receive packet filtering rules from the rule provider and a packet corresponding to at least one of the network-threat indicators. Based on packet-filtering rules, a packet filtering device will (1) determine that the packet corresponds to criteria specified by one of packet-filtering rules, (2) apply an operator (e.g., ALLOW or BLOCK) specified by the rule to the packet, (3) generate a log entry identifying threat indicators and corresponding

[80] '722 patent, at 4:30-38.
[81] '722 patent, at 4:65-5:4.

operator.[82] Log entries are communicated to the user via an interface and the user may reconfigure the operator associated with the rule as needed.[83]

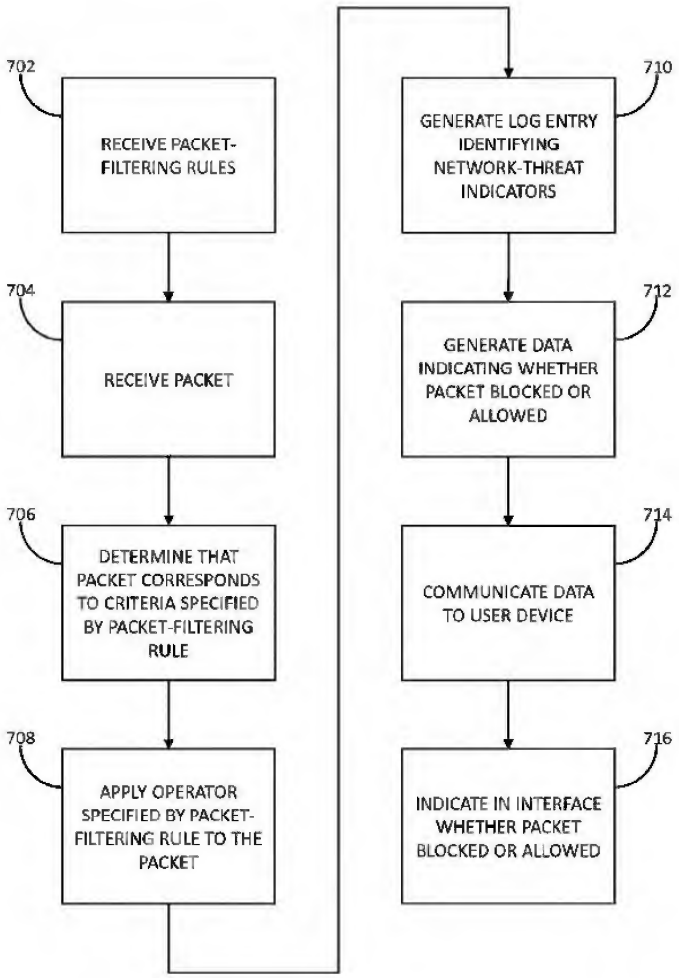


FIG. 7

Figure 54. An illustrative method for rule-based network-threat detection ('722 Patent, FIG.7).

[82] '722 patent, at 15:52-16-34.
[83] '722 patent, at 9:22-53.

B. THE ASSERTED SUBJECT MATTER OF THE '722 PATENT

344. I have been asked to assess whether the limitations of claims 1 and 25 recite generic computer components or well-known, routine, or conventional activities.

345. It is my opinion that the components recited in claims 1 and 25 are generic components. The '722 patent discloses that the claimed functionality is not limited to any specific computing device, and may instead be implemented on one or more generic and well-known computing devices:

> The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer-executable instructions and computer-usable data described herein ('722 Patent, 16:36-56.)

346. Further, in my opinion packet-filtering devices were well-known in the industry before the filing date of the '722 patent. Claim 1 recites a method performed by a packet-filtering device that applies packet filtering rules. As explained in the Technology Background section above, packet filtering devices have been well-known since the late 2000s. The PoliWall and

Check Point R77 systems were also well-known packet-filtering devices prior to the priority claim of the '722 patent, as discussed above.

347. In my opinion, the steps of claims 1 and 25 were also generic and conventional in the prior art before the '722 patent's filing date. I agree with Judge Morgan's observation in his November 2017 Order & Opinion (Dkt. 53) that the claims are written broadly and generically and generally relate to a packet filtering system that requires a human to instruct the system to block packets. For the reasons set forth above in my opinions regarding anticipation and obviousness of claims 1 and 25 of the '722 patent, the claim steps, both alone and in combination, were well-known and conventional in the field and in public use before the '722 patent's filing date.

C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF TIPPINGPOINT IPS

348. The TippingPoint UnityOne-200 Intrusion Prevention System ("TippingPoint IPS" or "TippingPoint system") is a network security solution to protect virtual and physical networks, applications, and data against a range of network security threats. This system performs the functions of two packet security gateways and one security policy management server, and a typical usage case for the system is to identify packets that correspond to criteria so that a criteria-specific action (e.g. blocking, logging, forwarding, re-routing, or the like) may be applied on a packet-by-packet basis to network traffic.

349. The TippingPoint system was commercially available to purchase prior to the priory date of the '722 Patent (see discussion above of priority dates).

350. For at least the reasons detailed below, it is my opinion that the TippingPoint system enabled a person of ordinary skill in the art to practice each and every element of Claims 1 and 25 of the '722 Patent, and that a POSITA would be motivated to do so as part of the

typical routine of setting up standard network protection mechanisms. Thus, it is also my opinion that the TippingPoint IPS anticipates these claims. In addition to the analysis presented herein, further discussion of relevant testing is described in Appendix D, which I incorporate by reference.

1. TEST CONFIGURATION WITH TIPPINGPOINT IPS

351. Exponent procured a TippingPoint IPS device with part number SBASY-199 Rev: C03 and serial number ST05170004, as shown in Figure 55.



Figure 55. TippingPoint IPS hardware showing the part number and serial number of the device.

352. The TippingPoint system includes a local security manager (LSM) program, which "is the control center from which you can configure, monitor, and report on the UnityOne

Intrusion Prevention System (IPS) devices in your network."[84] The TippingPoint IPS also includes two separate Ethernet port pairs called "segments"; each segment can be programmed to follow its own set of filtering rules via the LSM, and has its own pair of Ethernet port connections labeled "A" and "B" for both "SEG 1" and SEG 2" for the first and second segment, respectively.

353. The TippingPoint IPS LSM includes "a graphical user interface (GUI) that enables you to monitor and configure your UnityOne Intrusion Prevention System (IPS) using an ordinary web browser."[85] For Exponent's testing, a computer running Windows XP was connected via Ethernet cable to the MGMT Ethernet port of the TippingPoint IPS, which is indicated with red annotations in Figure 56, and Internet Explorer 7 was used to access the TippingPoint IPS GUI from this computer.[86]

---

84 "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. xi.

85 "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 8.

86 The TippingPoint IPS web server was found to be incompatible with modern versions of Internet Explorer. Internet Explorer 7 was released circa 2006. (See, for example, https://en.wikipedia.org/wiki/Internet_Explorer_version_history#Windows_Internet_Explorer_7.)



Figure 56. Annotated photographs of the TippingPoint IPS showing two packet security gateway interfaces (lower left) and one management interface (lower right).

354. The physical configuration of the test setup used for Exponent's analysis is shown in Figure 57. Only use of one segment, SEG 1, was required to demonstrate the method claimed by claims 1 and 25 of the '722 Patent. Computer A (IP address 192.168.1.46) is connected via Ethernet cable to the SEG 1-A TippingPoint port; and, Computer B (IP address 192.168.1.56) is connected via Ethernet cable to the SEG 1-B TippingPoint port. The laptop labeled "LSM" is the Windows XP machine that is used to access the LSM GUI and communicate with the TippingPoint IPS via the associated web server through the MGMT Ethernet port.

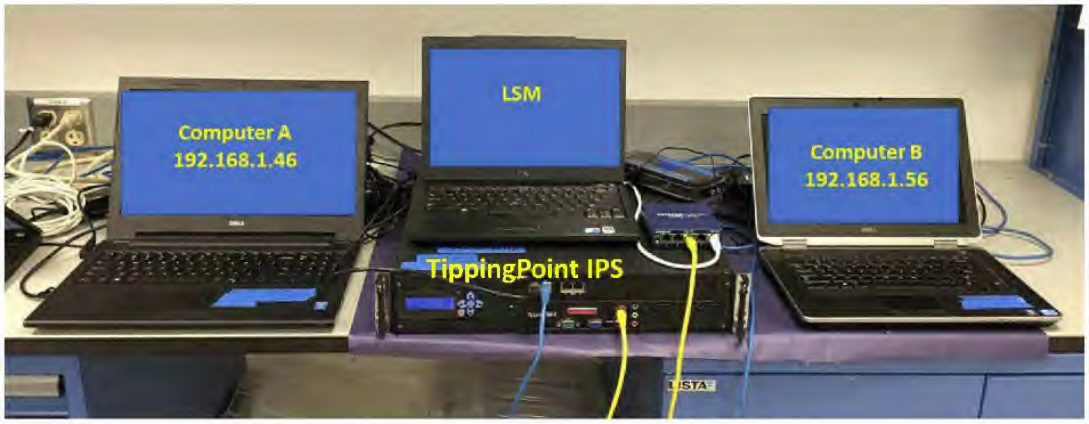


Figure 57. Test network including: (1) the TippingPoint IPS (center/bottom); (2) a Windows computer (labeled LSM) running the LSM GUI (web client) that is connected to the management interface (center/top); (3) a Linux computer (labeled Computer A) connected to the SEG1-A packet filter input/output port; (4) a Windows computer (labeled Computer B) connected to the SEG1-B packet filter input/output port.

355. Figure 58 shows a schematic layout of the network described above, depicting all three computers, their IP addresses, and all three Ethernet connections to the TippingPoint IPS.

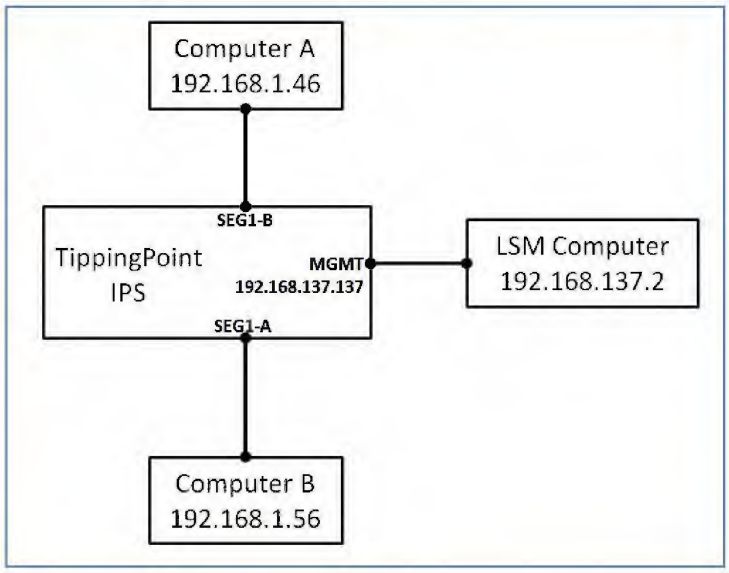


Figure 58. Network map of test network illustrating connectivity of TippingPoint IPS, Computer A, Computer B, and LSM Computer.

2. CLAIM 1

356. **Claim 1a: A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators.** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

357. The TippingPoint UnityOne-200 system ("TippingPoint IPS" or "TippingPoint system") is "an Intrusion Prevention System that provides a unified approach to network security."[87] The method by which the TippingPoint IPS provides network security involves filtering packets by applying a set of user-defined filters. As detailed below, the method by which the TippingPoint system operates satisfies all requirements of element claim 1a of the '722 Patent.

358. I understand that the parties have agreed that the term "network-threat indicators" is to be construed as "indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like," and I have applied this claim construction throughout my analysis.

359. I also understand that there is a dispute regarding the construction of the term "packet-filtering device." More specifically, Plaintiffs have proposed that this term be construed as "a device programmed to filter packets based on data associated with a packet," while Defendants have proposed that no construction is needed and that this term should be given its "plain meaning." I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction

---

87 "TippingPoint IPS Hardware Installation and Safety Guide v 2.5.4" (copyright 2008) at p. xi.

should be applied. Regardless of which construction is applied, the TippingPoint system comprises a "packet-filtering device," as explained below.

360. I also understand that there is a dispute regarding the construction of the term "packet-filtering rules." More specifically, Plaintiffs have proposed that this term be construed as "condition or set of condition that when satisfied cause a computing device to filter packets based on data associated with a packet," while Defendants have proposed "(i) packet-identifying criteria and (ii) an operator to be performed on the identified packets." I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint IPS receives "a plurality of packet-filtering rules," as detailed below.

361. The TippingPoint system is intended to be located at the interface between two different machines or networks, such that packets sent between said machines or networks must pass through the TippingPoint IPS. For example, in the test configuration described above, the TippingPoint IPS is located between Computers A and B such that packets are not sent directly between these machines, but rather are first received by the TippingPoint IPS which then in turn can pass the communication to its intended destination. More specifically: packets sent from Computer A to Computer B are received by the TippingPoint IPS via Ethernet port SEG 1-A, and then can be forwarded to Computer B via TippingPoint IPS Ethernet port SEG 1-B; similarly, packets sent from Computer B to Computer A are received by the TippingPoint IPS via Ethernet port SEG 1-B, and then can be forwarded to Computer A via TippingPoint IPS Ethernet Port SEG 1-A. The TippingPoint system does not have to forward all packets, however, and can instead perform a variety other functions, such as

dropping, logging, tracing, rerouting, to packets that match certain criteria. The criteria for identifying packets, and the functions that are performed on said packets, are determined using a set of filters that are configured by a user via the LSM GUI and communicated to the TippingPoint ISP via the associated web server. Each filter comprises at least one rule, which specifies at least one criteria used to determine which packets are subject to the at least one rule, and at least one function that is to be performed on such packets. Thus, at least because the TippingPoint IPS is programmed with filters that filter packets according to criteria that may be based on data associated with the packet (such as IP addresses, URLs, packet data content, etc.) the TippingPoint IPS constitutes a "device programmed to filter packets based on data associated with a packet," which satisfies Plaintiff's proposed construction for "packet-filtering device." Also, in my opinion, a POSITA would recognize that the "plain meaning" for "packet-filtering device" is also satisfied by the TippingPoint IPS, at least because the TippingPoint IPS is a device that filters packets, and thus Defendants' proposed construction for "packet-filtering device" is also satisfied. Also, I note that each filter causes the TippingPoint ISP to filter packets based on data associated with each packet, at least because the TippingPoint ISP applies filters only to packets that match the applicable condition or conditions of the criteria of said filter: thus the filters satisfy Plaintiff's proposed construction for "packet-filtering rules." Similarly, at least because each filter comprises a criteria, which constitutes "packet-identifying criteria" and a function to be performed on matching packets, which constitutes "an operator to be performed on the identified packets," the filters satisfy Defendants' proposed construction for "packet-filtering rules."

362. Exponent has demonstrated that the TippingPoint system operates a method in which the TippingPoint IPS packet-filtering device receives "a plurality of packet-filtering rules

configured to cause the packet filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators," as detailed below.

363. A well-known example of a network-threat indicator is a packet or set of packets that are associated with unauthorized attempts to access sensitive data: any packet that is part of an attempt to retrieve sensitive data may constitute a network-threat indicator unless the requesting machine is trusted and communication with said requesting machine is secure. Packets from untrusted/unknown sources that are attempting to access a sensitive file satisfy the agreed claim construction for "network-threat indicators," at least because the network addresses and URLs therein are associated with the network-threat that the sensitive file may be accessed without proper authorization. Passwords are often considered to be sensitive data, at least because they can grant access to important functions or files. A typical location in which passwords for UNIX systems can be stored is the file /etc/passwd. Thus packets that are associated with access requests for this file are often regarded as network threats. The TippingPoint system includes a filter for identifying packets that are attempting to access the /etc/passwd file: the *0361:HTTP:Protected File Access (/etc/passwd)* filter. Figure 59 shows a screenshot from the TippingPoint LSM GUI of a screen used to configure the *0361:HTTP:Protected File Access (/etc/passwd)* filter. The "Action" setting enables the user to set the function that will be performed upon packets that are attempting HTTP requests to access file /etc/passwd, and is currently set to "Permit + Notify" in the screenshot: with this configuration, the TippingPoint system forwards matching packets, but also creates a corresponding entry within an Alert Log to serve as notification that such packets have been detected.

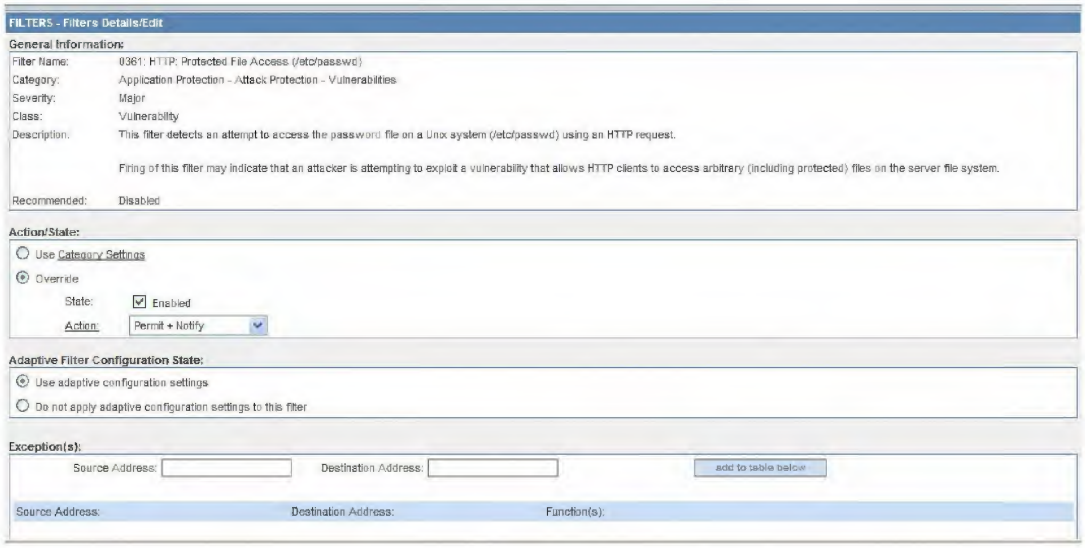


Figure 59. Screenshot from the TippingPoint Local Security Manager (LSM) graphical user interface88 display of the description of filter "0361," which "detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request."

364. A HTTP GET request for the URL /etc/passwd was sent by Computer A to Computer B with the *0361:HTTP:Protected File Access (/etc/passwd)* filter installed and configured as shown in Figure 59, this process is discussed in more detail in relation to subsequent claim elements below. Figure 60 shows a screenshot of the TippingPoint system Alert Log in which a corresponding log entry has been placed to record the packet that matched the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter. Thus, this demonstrates that the TippingPoint IPS packet-filtering device can receive a packet-filtering rule that is configured to cause the TippingPoint IPS packet-filtering device to identify packets corresponding to a network-thread indicator.

88 See, generally, "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005).



Figure 60. Screenshot from the TippingPoint LSM GUI showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was allowed.

365. Furthermore, the TippingPoint system is not limited to receiving a single packet filtering rule, but can in fact receive a plurality of such rules. Figure 61 shows a screenshot from the TippingPoint LSM GUI that shows 15 of the over 1000 filters that are available on the TippingPoint system via default.

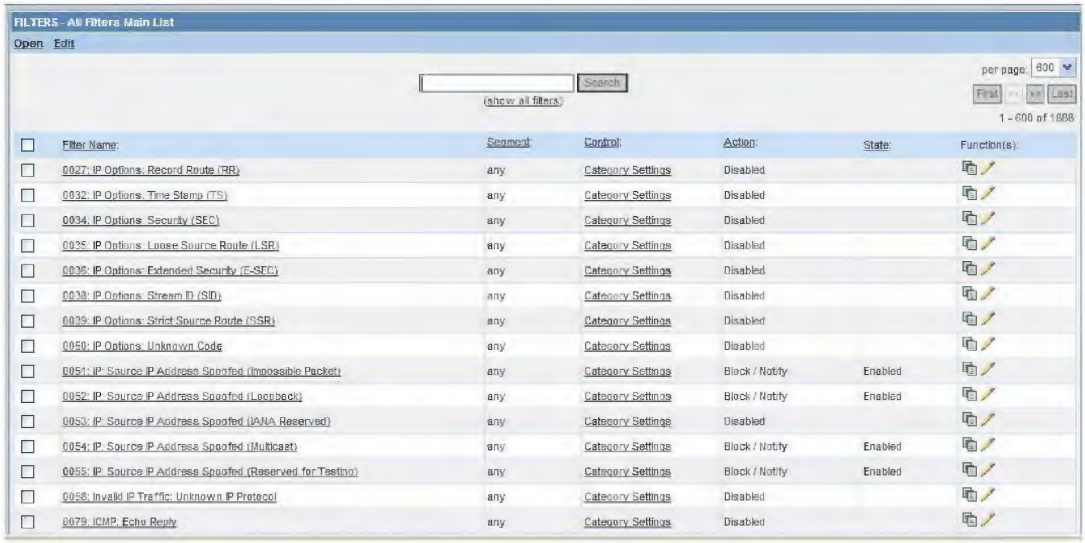


Figure 61. Screenshot from the TippingPoint LSM graphical user interface display of available filters and their current state of implementation

366. Using a combination of filters, the TippingPoint system "provides … monitoring and managing packets while blocking malicious attacks … provides total packet inspection … integrates Intrusion Prevention, Stateful IP Filtering (traffic management filters), and

network discovery security applications." [89] Also, the TippingPoint IPS "detects and blocks inappropriate, incorrect, or anomalous activity on the network by comparing network traffic with *filters*..."[90] (emphasis in original). Thus, for at least the reasons above, the TippingPoint system performs a method that satisfies all requirements of element 1a of the '722 Patent.

367. Therefore, for at least the reasons above, it is my opinion that the TippingPoint system anticipates element 1a of the '722 Patent.

368. **Claim 1b: receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet.** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

369. The TippingPoint IPS is located at an interface between networks or between machines, such that all packets traveling between these networks or machines are received by the TippingPoint system. Thus, the TippingPoint system satisfies the requirements of this claim element at least because, as detailed above, the TippingPoint IPS constitutes a "packet-filtering device" according to the relevant claim constructions, and said packet-filtering device receives many more than two packets during any typical, practical use.

370. By way of a more specific example, Exponent has explicitly demonstrated that the TippingPoint system performs a method that includes the TippingPoint IPS receiving a first packet and a second packet, as detailed below.

371. In the example demonstration of the *0361:HTTP:Protected File Access (/etc/passwd)* filter discussed in relation to claim element 1a, the "Action" to be performed on packets that

---

89 "TippingPoint IPS Hardware Installation and Safety Guide v 2.5.4" (copyright 2008) at p. 1.
90 "TippingPoint IPS Hardware Installation and Safety Guide v 2.5.4" (copyright 2008) at p. 1.

were attempting access to /etc/passwd was set to "Permit + Notify," which causes the TippingPoint system to forward matching packets while also creating a corresponding entry in an Alert Log.

372. To demonstrate this functionality, using the system described above in relation to Figure 57 and Figure 58, a HTTP server was hosted[91] on Computer B at IP address 192.168.1.56 on port 8000, and a program called "netcat"[92] was used to send a HTTP GET request for the URL path /etc/passwd from Computer A to Computer B. Figure 62 shows a screenshot from Computer A that displays the netcat GET request (netcat is invoked via the "nc" command), along with the HTTP response from the web server on Computer B indicating that the file was not found. Similarily, Figure 63 shows a screenshot from Computer B that shows the arrival of the GET request for the path /etc/passwd generates a HTTP code 404 response from the HTTP server because file /etc/passwd is not found. This is the expected response, because a /etc/passwd was not created on Computer B. Thus, testing described above demonstrates that a HTTP GET request was successfully forwarded from Computer A to Computer B, and the resulting 404 error response was successfully forwarded from Computer B to Computer A.

---

91 Python was used, via a python language interpreter and standard python module called "http.server," to run an HTTP server on Computer B. For additional information, see https://docs.python/org (generally) as well as https://docs.python.org/2/library/simplehttpserver.html and https://docs.python.org/3/library/http.server.html.

92 Netcat is a well-known utility, see, for example, http://netcat.sourceforge.net/ and https://nmap.org/ncat/.

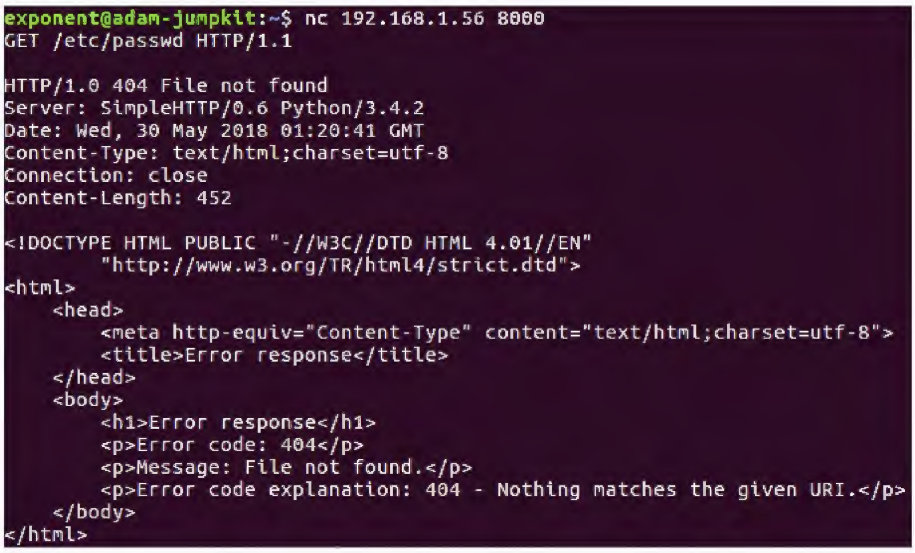


Figure 62. Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, the HTTP GET request for the "/etc/passwd" path, and the response from Computer B indicating that the "etc/passwd" file was not found by the server (thus it responds with a 404 error).

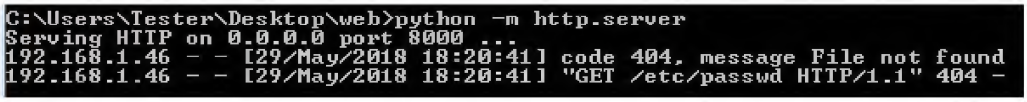


Figure 63. Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server has sent back an HTTP code 404 in response to the GET request for "/etc/passwd."

373. That the TippingPoint system identified the above HTTP GET request is confirmed by the creation of a corresponding entry in the Alert Log, which is shown above in relation to claim element 1a in Figure 60. This HTTP GET request packet constitutes an example "first packet," as required by claim element 17b.

374. The TippingPoint LSM GUI was subsequently used to alter the configuration of the *0361:HTTP:Protected File Access (/etc/passwd)* filter such that the "Action" that will be performed on matching packets was changed from "Permit + Notify" to "Block + Notify," as

shown in Figure 64. When configured to "Block + Notify," the filter results in matching packets being dropped, and a corresponding entry being created in a Block Log.

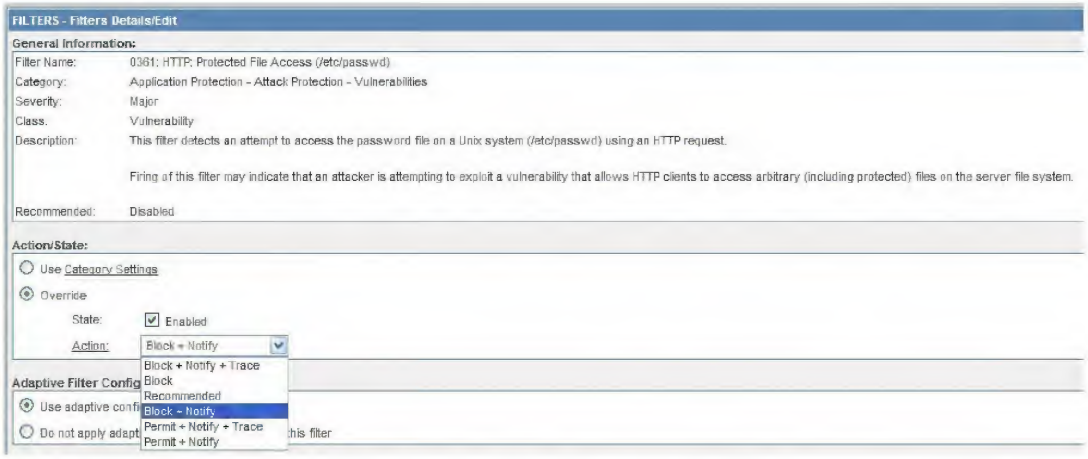


Figure 64. Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from "Permit + Notify" to "Block + Notify."

375. With the *0361:HTTP:Protected File Access (/etc/passwd)* filter configured to "Block + Notify," a second HTTP GET request for the URL path /etc/passwd was sent by Computer A to Computer B. Figure 65 shows a screenshot from Computer A showing this second HTTP GET request: the "^C" indicates that the HTTP client was forcibly shutdown via using "Ctrl+C" on the keyboard to send the client a kill signal. This was required due to the absence of any HTTP response from the web server on Computer B.

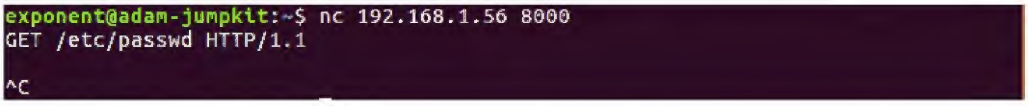


Figure 65. Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, and the HTTP GET request for the "/etc/passwd" path. It also illustrates that no response was received from Computer B (because Computer B never received the request).

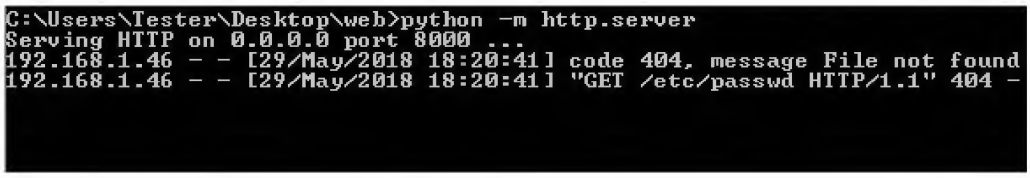


Figure 66. Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server did not send back any additional response because it did not receive the second packet. (The response shown in the figure is the response to the first packet.).

376. Also, Figure 66 shows a screenshot from Computer B during the second HTTP GET request: no additional output was caused by this second HTTP GET request because the TippingPoint system dropped the associated packet from Computer A and thus Computer B did not receive a second request.

377. In addition, as shown in the screenshot of the Block Log in Figure 70, the second HTTP GET request packet was indeed blocked by the TippingPoint system, as verified by the creation of a corresponding entry in the Block Log. Note also the "Date/Time" field of the Block Log, which shows a time that is approximately two minutes later than the time at which the first packet was logged in the Alert Log as shown in Figure 60. Thus, the second, blocked, HTTP GET request constitutes a "second packet," as required by claim element 1b.

.



Figure 67. Screenshot from the TippingPoint LSM GUI, showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was blocked.

378. Thus, as demonstrated above, the TippingPoint system performs a method that satisfies all requirements of claim element 17b of the '722 Patent.

379. Therefore, for at least the reasons above, it is my opinion that claim element 17b of the '722 is anticipated by the TippingPoint system.

380. **Claim 1c: responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators: applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet.** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

381. I understand that there is a dispute regarding the construction for "responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators." More specifically, Plaintiffs have proposed that this term be construed as "if the packet-filtering device determines the first packet meets one or more conditions associated with one or more network threat indicators from a packet filtering rule," while Defendants propose that no construction is needed and this term should be given its "plain meaning." I have considered both proposed construction in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which

construction is applied, the TippingPoint system satisfies all requirements of claim element 1c, for at least the reasons below.

382. I also understand that there is a dispute regarding the construction of the term "operator." More specifically, Plaintiff has proposed that this term be construed as "an adjustable instruction that causes the packet filtering device to either prevent or allow a packet to continue to a destination," while Defendants have proposed that this term be construed as "function to either prevent a packet corresponding to criteria from continuing or allow it to continue to its destination." I have considered both proposed claim constructions in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of claim element 1c, for at least the reasons below.

383. As described in detail in relation to claim elements 1a-b, Exponent has demonstrated the the *0361:HTTP:Protected File Access (/etc/passwd)* filter in conjunction with a "first packet" and a "second packet." During the above-described demonstration, both the first packet and second packet constituted a "network threat indicator" and satisfied the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter. For the first packet, this filter was set to "Permit + Notify," which caused the filter to cause the TippingPoint IPS to allow the first packet to continue towards its destination, while also creating a corresponding entry in an Alert Log. Thus, the first packet in the above-described demonstration, and its interaction with the TippingPoint system, satisfies all requirements of claim element 1c.

384. More specifically, in view of Defendants' proposed claim construction "if the packet-filtering device determines the first packet meets one or more conditions associated with one or more network threat indicators from a packet filtering rule," this proposed construction has

been satisfied by the above-described demonstration at least because: (1) the *0361:HTTP:Protected File Access (/etc/passwd)* filter is only applied if the TippingPoint IPS determines that the first packet meets the associated conditions, i.e. that said packet is attempting to access /etc/passwd; (2) the associated conditions correspond to a network threat indicator, at least because accessing /etc/passwd is generally considered to be accessing sensitive data.

385. Also, the above-described demonstration satisfies both parties' proposed constructions for "operator": Regarding Plaintiff's construction, the "Action" performed upon packets that match the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter constitutes "an adjustable instruction that causes the packet filtering device to either prevent or allow a packet to continue to a destination" at least because the "Action" can be adjusted to either allow or prevent matching packets from continuing to their destination; regarding Defendant's construction, the "Action" constitutes a "function to either prevent a packet corresponding to criteria from continuing or allowing it to continue to its destination" at least because said "Action" can be set such that the filter either prevents or allows packets that correspond to the filter criteria to reach their destination.

386. Thus, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1c.

387. Therefore, for at least the reasons above, it is my opinion that claim element 1c is anticipated by the TippingPoint system.

388. **Claim 1d. communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the**

first packet; As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

389. I understand that there is a dispute regarding the construction for the term "communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet." More specifically, Plaintiff has proposed that this term be construed as "causing a packet-filtering device to generate and communicate a record that identifies (1) a network threat indicator based on a rule and (2) data that indicates that the first packet was allows to continue toward the destination," while defendants have proposed that no construction is required and this term should be given its "plain meaning." I have considered both proposed claim constructions in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of this claim, as detailed below.

390. The demonstration described above in relation to claim elements 1a-b verifies that the TippingPoint system satisfies all requirements of claim element 1d: More specifically, the Alert Log shown in Figure 60 demonstrates that the TippingPoint system satisfies all requirements of this claim element. Note, for the TippingPoint LSM GUI to display this log information, the TippingPoint IPS must have communicated this information to a data store served by the web server running on the TippingPoint IPS interface because it is this web server that servers the content that is viewable via the TippingPoint LSM GUI. Thus, this log constitutes the TippingPoint IPS communicating information from the *0361:HTTP:Protected File Access (/etc/passwd)* filter that identifies which filter generated the log entry (and thus

identifies the associated network-threat indicators that correspond to this filter), and the fact that the entry is in the "Alert Log" communicates that the packet was allowed to continue toward its destination because the Alert Log is used to log only packets that were forwarded. Thus, the plain meaning of the requirements of this claim, as would be understood by a POSITA, have been satisfied by the demonstration presented in relation to claim elements 1a-b.

391. Plaintiff's proposed claim construction is also satisfied by the above-described demonstration, at least because the TippingPoint ISP segment 1, which constitutes a "packed-filtering device" has generated and communicated a record that: (1) includes the particular filter that caused the record to be generated, which contains the network threat indicator upon that said filter responds to; and (2) all entries in the Alert Log correspond to packets that were allowed to continue toward their destination, thus the fact that an entry was created in the Alert Log constitutes a record that indicates that the data packet was allows to continue towards its destination, i.e. part of the communication from the TippingPoint ISP segment 1 to the web server data store associated with the TippingPoint LSM must necessarily identify that the corresponding record is to be entered into the Alert Log, and thus this part of the communication satisfies requirement (2) of Plaintiff's proposed construction relevant to this claim.

392. Thus, for at least the reasons above, it the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1d.

393. Therefore, for at least the reasons above, it is my opinion that element 1d is anticipated by the TippingPoint system.

394. **Claim 1e: causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

395. I understand that there is a dispute regarding the construction for "interface." More specifically, Plaintiff has proposed that this term be construed as "plain and ordinary meaning," while Defendants have proposed that this term be construed as "a display visible to the user that allows a user to provide input." I have considered both proposed constructions in my analysis, and I reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of claim element 1e, as detailed below.

396. As described above in relation to claim element 1d, the Alert Log picture in Figure 60 satisfies the requirements of claim element 1e. More specifically, this Alert Log forms part of the system interface and displays information corresponding to the packet-filtering rules, such as the filter used for the above-described demonstration. The Alert Log is displayed on the TippingPoint LSM GUI, that was viewed during testing via the screen on a laptop (see Figure 57). The TippingPoint LSM GUI enables a user to interact with the TippingPoint system, e.g. view and amend settings, view logs, etc., and thus satisfies the plain and ordinary meaning for the term "interface" as would be understood by a POSITA. Also, the TippingPoint LSM GUI constitutes "a display visible to the user that allows a user to provide input," as least because a user is able to see said GUI and use it to alter the filter settings as demonstrated above in relation to claim elements 1a-c. Therefore, both Plaintiff's and

Defendants' proposed constructions for "interface" are satisfied by the TippingPoint LSM GUI.

397. Thus, for at least the reasons above, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1e.

398. Therefore, for at least the reasons above, it is my opinion that claim element is anticipated by the TippingPoint system.

399. **Claim 1f: receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and.** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

400. I understand there is a dispute regarding the construction of the term "user." More specifically, Plaintiff has proposed that this term be given its "plain and ordinary meaning," while defendants have proposed that this term be construed as "person (e.g., administrator)." I have considered both claim constructions in my analysis, and reserve the right to modify my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of this claim. In any event, it is my opinion that the plain and ordinary meaning of the term "user" includes "person (e.g., administrator).

401. As described in relation to claim elements 1a-c, Exponent has demonstrated that the TippingPoint system satisfies all requirements of claim element 1f. More specifically, the TippingPoint security gateway segment 1 constitutes a packet-filtering device, and has been demonstrated to receive instructions generated in response to a user, such as a person,

invoking a selection within the dropdown menu of the settings for the *0361:HTTP:Protected File Access (/etc/passwd)* filter: this settings window is shown, for example, in Figure 64, in which the dropdown menu that comprises "an element in the at least one portion of the interface" is shown. As detailed in relation to elements 1a-c, this "Action" dropdown menu corresponds to the function that will be performed by the *0361:HTTP:Protected File Access (/etc/passwd)* filter upon packets that match the associated network-threat indicator, which for this filter is packets that attempt to access the /etc/passwd file. That invoking the "Action" dropdown menu shown in Figure 64 results in the TippingPoint IPS receiving an instruction was demonstrated in relation to claim elements 1b, where altering the dropdown menu selection from "Permit + Notify" to "Block + Notify" altered the behavior of the TippingPoint IPS by changing the function applied to packets that matched the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter.

402. Thus, for at least the reasons above, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1f.

403. Therefore, for at least the reasons above, it is my opinion that claim element 1f is anticipated by the TippingPoint system.

404. **Claim 1g: responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and.** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

405. I understand that there is a dispute regarding the construction of the term "modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to

reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their destination." More specifically, Plaintiff has proposed that this term be construed as "modifying the state of the packet-filtering device to cause an adjustable instruction to prevent a packet from continuing toward its destination," while Defendants propose that no construction is required and this term should be given its "plain meaning." I have considered both proposed constructions in my analysis, and I reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of claim element 1g, as detailed below.

406. As described in relation to claim elements 1a-c, Exponent has demonstrated that the TippingPoint system satisfies all requirements of claim element 1f. More specifically, a first packet that corresponded to the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter was demonstrated to be permitted to reach its final destination when the "Action" setting for said filter was set to "Permit + Notify"; however, when the "Action" setting was subsequently changed using the TippingPoint LSM GUI to "Block + Notify," a second packet that corresponded to the same criteria was prevented from continuing towards its destination. This demonstrates that the operator performed by the *0361:HTTP:Protected File Access (/etc/passwd)* filter was modified in response to the TippingPoint IPS receiving an instruction from the TippingPoint LSM GUI, and that this modification was to prevent packets corresponding to a criteria from continuing toward their destination. Thus, the "plain meaning" of this claim element, as would be understood by a POSITA, has been demonstrated as being satisfied by the TippingPoint system.

407. Plaintiff's proposed claim construction of relevance to this claim element is also satisfied by the above-described demonstration. More specifically, the "Action" associated with the *0361:HTTP:Protected File Access (/etc/passwd)* filter constitutes "an adjustable instruction" and setting this to "Prevent + Notify" constitutes "modifying the state of the packet-filtering device to cause an adjustable instruction to prevent a packet from continuing toward its destination."

408. Thus, for at least the reasons above, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1g.

409. Therefore, for at least the reasons above, it is my opinion that claim element 1g is anticipated by the TippingPoint system.

410. **Claim 1h: responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria: preventing by the packet-filtering device, the second packet from continuing toward a destination of the second packet;** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

411. As described in relation to claim elements 1a-c, Exponent has demonstrated that the TippingPoint system satisfies all requirements of claim element 1f. More specifically, the TippingPoint IPS security gateway segment 1, which constitutes the "packet-filter device," was demonstrated to determine that a second packet corresponded to the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter, and prevented this packet from continuing towards its destination. That the TippingPoint IPS determined the second packet matched the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter was confirmed via inspection of the Block Log, which included an entry corresponding to the

determination that the criteria of the *0361:HTTP:Protected File Access (/etc/passwd)* filter were satisfied; that the second packet was prevent from reaching its destination was confirmed by the fact that Computer B did not register receipt of the second packet, and Computer A did not receive any response to the packet.

412. Thus, for at least the reasons above, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1h.

413. Therefore, for at least the reasons above, it is my opinion that claim element 1h is anticipated by the TippingPoint system.

414. **Claim 1i: communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and.** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

415. As described in relation to claim elements 1a-c, Exponent has demonstrated that the TippingPoint system satisfies all requirements of claim element 1f. More specifically, the Block Log shown in Figure 67 confirms that, in addition to blocking the second packet, the TippingPoint IPS security gateway segment 1 also communicated data indicative that the second packet was blocked to the data store of the web server associated with the TippingPoint LSM. This is known because the TippingPoint LSM GUI displays information retrieved from the associated web server, so in order for the entry shown in Figure 67 to be displayed the TippingPoint ISM must necessarily have communicated data indicative that the corresponding packet was blocked to the data store of the web server. That the TippingPoint IPS has sent an entry to the Block Log is communicative that the corresponding packet was blocked.

416. Thus, at least for the reasons above, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1i.

417. Therefore, for at least the reasons above, it is my opinion that claim element 1i is anticipated by the TippingPoint system.

418. **Claim 1j: causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.** As detailed below, the TippingPoint system performs a method that satisfies all requirements of this claim element.

419. As described in relation to claim elements 1a-c, Exponent has demonstrated that the TippingPoint system satisfies all requirements of claim element 1f. More specifically, the Block Log shown in Figure 67 constitutes an interface that includes "display of the data indicative that the second packet was prevented from continuing towards" its destination, at least because all entries in the Block Log correspond to packets that were prevented from continuing toward their destination.

420. Thus, for at least the reasons above, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1j.

421. Therefore, at least for the reasons above, it is my opinion that claim element 1j is anticipated by the TippingPoint system.

422. For at least the reasons detailed above, it is my opinion that the TippingPoint system satisfies each and every limitation of claim 1 of the '722 Patent. Consequently, for at least the reasons above, it is my opinion that claim 1 of the '722 Patent is anticipated by the TippingPoint system.

3. CLAIM 25

423. **Claim 25: The method of Claim 1, wherein: receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices.** This claim is dependent upon claim 1 of the '722 Patent, and as detailed above it is my opinion that claim 1 is anticipated by the TippingPoint system. As detailed below, the TippingPoint system also satisfies all limitations added to claim 1 of the '722 Patent by claim 25 therein.

424. As detailed in relation to claim 1, each TippingPoint segment constitutes a "packet-filtering device" as required by claim 25 and the relevant claim constructions; and, also as detailed in relation to claim 1, the filters used by the TippingPoint system constitute "packet-filtering rules" as required by claim 25 and the relevant claim constructions. The TippingPoint IPS (specifically, the UnityOne-200 model) supports two different "segments" named SEG1 and SEG2. Although only one TippingPoint segment, SEG 1, was required for demonstrating that the TippingPoint system satisfies the method of claim 1, the limitations added by claim 25 require use of more than one packet-filtering device. This was achieved by extending the test configuration to make use of SEG 2 of the TippingPoint system. Figure 68 shows the physical hardware used to demonstrate that the TippingPoint system satisfies all requirements added to claim 1 by claim 25.

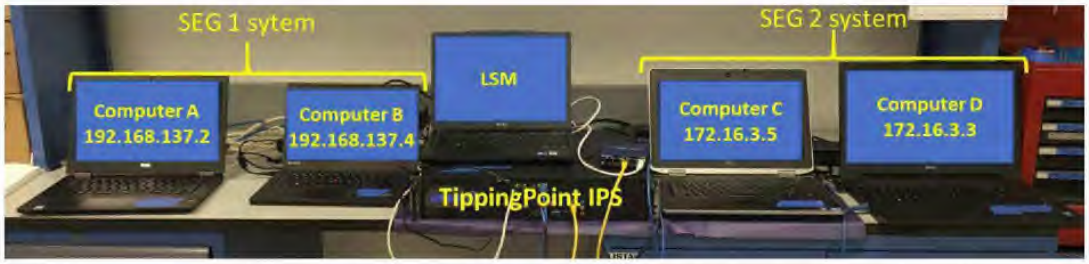


Figure 68. Annotated photograph of test network used in Claim 25 analysis.

The network used to demonstrate the requirements of claim 1 has been extended to includes two more computers: Computer C (IP address 172.16.3.5) is connected to the SEG 2-A Ethernet port; and Computer D (IP address 172.1.3.3) is connected to the SEG 2-B Ethernet port. Figure 72 shows a schematic representation of the extended network.

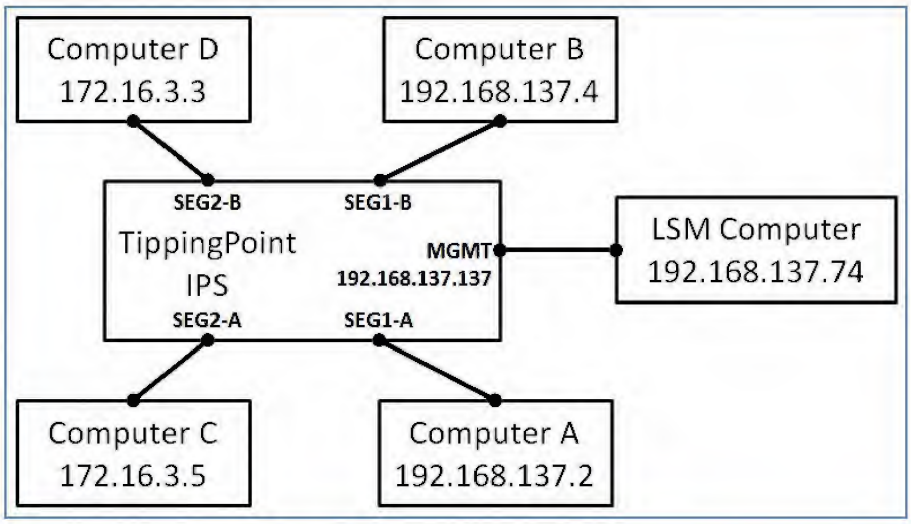


Figure 69. Network map for the test network used in the analysis of Claim 25.

425. Both TippingPoint segments can be configured via the TippingPoint LSM GUI and associated web server. Each TippingPoint segment can be independently programmed, e.g. a different set of filters can be installed on each segment, or the settings of a given filter that is installed on both segments can be configured differently for each segment. Thus, at least because each TippingPoint segment has the same functionality, each segment can perform

the demonstration detailed in relation to claim 1. Consequently, the TippingPoint system satisfies the limitations added to claim 1 by claim 25, at least because the TippingPoint system performs the method of claim 1 and can do so using either, or both, of its segments.

426. More specifically, the TippingPoint LSM running on the laptop connected to the TippingPoint IPS via the associated web server constitutes "one or more computing devices" that, in the same way as demonstrated in relation to claim 1 for TippingPoint segment 1, can "provide packet-filtering rules" to both TippingPoint segment 1 and TippingPoint segment 2; and, each of these TippingPoint segments is able to perform the demonstration discussed in relation to claim 1 and is thus able to perform the method of claim 1.

427. As a demonstration of the above, Exponent has used the TippingPoint LSM GUI to independently program TippingPoint segments 1 and 2 to independently configure the *0361:HTTP:Protected File Access (/etc/passwd)* filter for each segment, as detailed below.

428. Initially, both *0361:HTTP:Protected File Access (/etc/passwd)* filters were set to "Permit + Notify" and a single packet was passed through each TippingPoint segment. Figure 70 shows the resulting Alert Log that lists two entries corresponding to these packets: the top entry (Log ID of 31) corresponds to the packet passed through Segment 1; and the bottom entry (Log ID of 30) corresponds to the packet passed through Segment 2. Both the entries in the Alert Log are identified as being the result of the *0361:HTTP:Protected File Access (/etc/passwd)* filter, and, as discussed in relation to claim 1, the existence of an entry in the Alert Log necessitates that a packet was identified as matching the criteria of the associated filter but as allowed to continue to its destination.

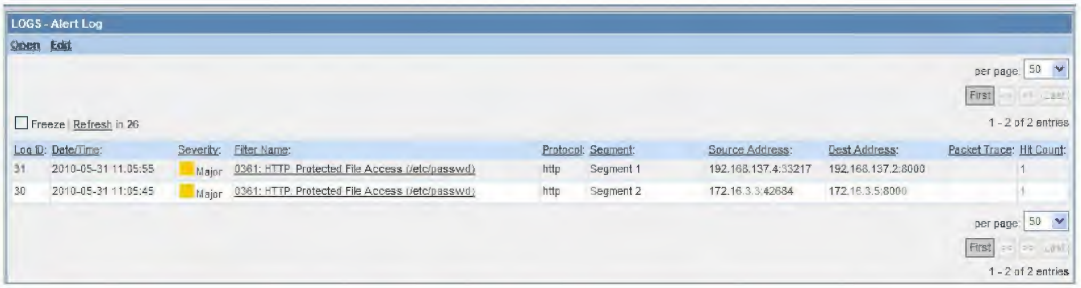


Figure 70. Screenshot from LSM GUI showing the Alert Log. Note that the upper log entry is for Segment 1 and the lower log entry is for Segment 2.

429. Both the *0361:HTTP:Protected File Access (/etc/passwd)* filters were subsequently set to "Block + Notify," and a single packet was passed through each TippingPoint segment. Figure 71 shows the resulting Block Log that lists two entries corresponding to these packets: the top entry (Log ID of 44) corresponds to the packet passed through Segment 1; and the bottom entry (Log ID of 43) corresponds to the packet passed through Segment 2. Both the entries in the Block Log are identified as being the result of the *0361:HTTP:Protected File Access (/etc/passwd)* filter, and, as discussed in relation to claim 1, the existence of an entry in the Block Log necessitates that a packet was identified as matching the criteria of the associated filter and was prevented from continuing towards its destination.

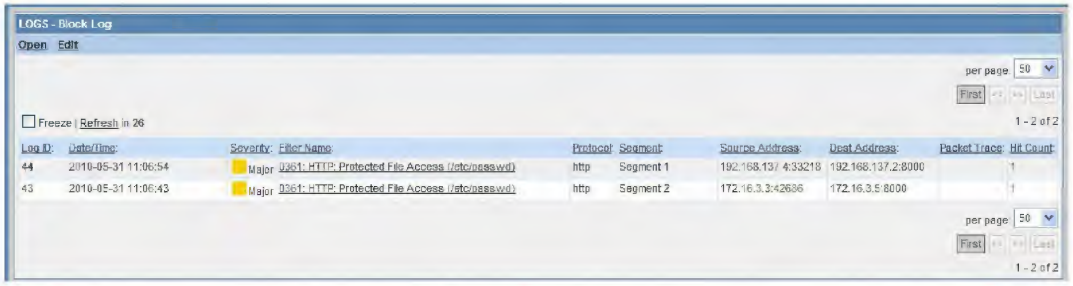


Figure 71. Screenshot from LSM GUI showing the Block Log. Note that the upper log entry is for Segment 1 and the lower log entry is for Segment 2.

430. To demonstrate independent programming of each TippingPoint segment, the *0361:HTTP:Protected File Access (/etc/passwd)* filter for segment 1 was set to "Block +

Notify" while the *0361:HTTP:Protected File Access (/etc/passwd)* filter for segment 2 was set to "Permit + Notify." This was achieved using the "Global Category Settings Table," shown in Figure 72, that enables the "Action" of all filters within a given segment to be set simultaneously.[93] Although the Global Category Settings Table was used for the testing described herein, it is also possible to individually configure the settings for each filter on each segment independently.

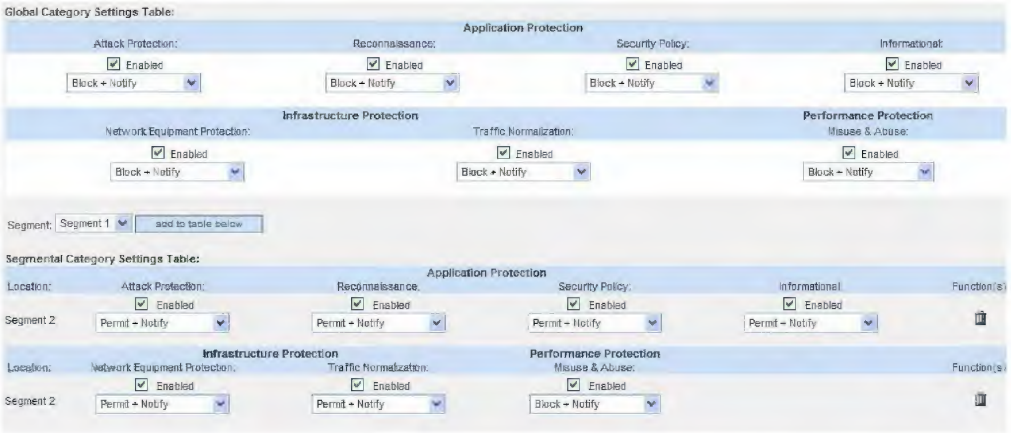


Figure 72. Screenshot from LSM GUI showing "Block + Notify" settings for Segment 1 and "Permit + Notify" settings for Segment 2.

431. Figure 73 and Figure 74 show the Block Log and Alert Log, respectively, after a single packet was sent through each TippingPoint segment when the settings shown in Figure 72 were in active: the Block Log contains a single entry corresponding to a packet identified by the *0361:HTTP:Protected File Access (/etc/passwd)* filter on segment 1; the Alert Log contains a single entry corresponding to a packet identified by the *0361:HTTP:Protected File Access (/etc/passwd)* filter on segment 2. Thus, TippingPoint segment 1 prevented the packet from continuing towards its destination, while TippingPoint segment 2 allowed the packet to

[93] Note that the "Performance Protection: Misuse and Abuse" is not able to be set to "Permit + Notify" option, and so remains set to "Block + Notify" for segment 2.

continue towards its destination. This demonstrates independent control of both TippingPoint segments from the TippingPoint LSM GUI.



Figure 73. Screenshot from LSM GUI showing that the HTTP: Protected File Access threat packet was blocked on Segment 1.



Figure 74. Screenshot from LSM GUI showing that the HTTP: Protected File Access threat packet was allowed on Segment 2.

432. Thus, for at least the reasons above, the TippingPoint system has been demonstrated to satisfy all requirement of claim 1 of the '722 Patent as well as all requirements added to this claim by claim 25 therein.

433. Therefore, at least for the reasons above, it is my opinion that the TippingPoint system anticipates claim 25 of the '722 Patent.

D. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF CHECK POINT R77

434. The Check Point R77 Security Gateway (SG)[94] performs the function of a packet-filtering device, and the Check Point R77 Security Management Server (SMS)[95] performs the

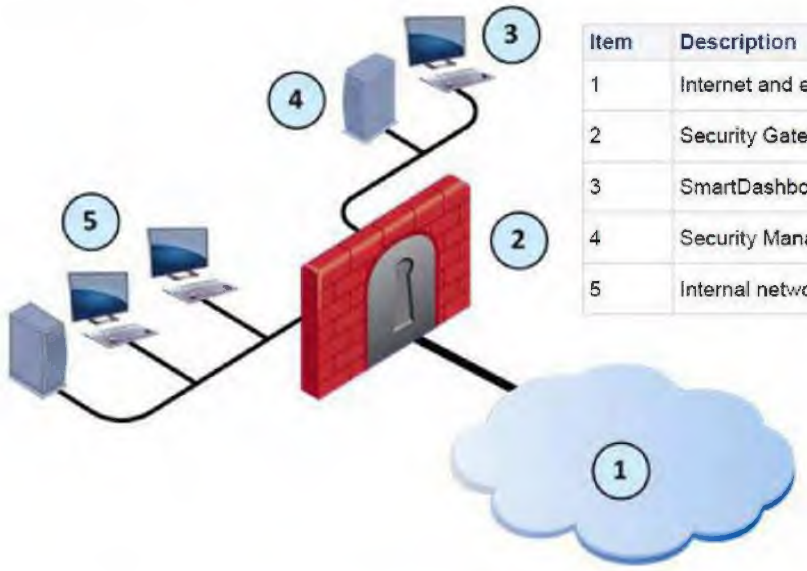
[94] See "Check Point R77 Firewall Administration Guide" (dated Aug 27, 2013).
[95] See "Check Point R77 Security Management Server Administration Guide" (dated Aug 27, 2013).

CENTRIPETAL-CSCO 087665

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 165

function of a security policy management server, which is a centralized server for managing packet-filtering rules and packet-filtering devices

435. An illustration of how the R77 SG and R77 SMS fit into a typical network architecture is shown in Figure 75.



Item	Description
1	Internet and external networks
2	Security Gateway
3	SmartDashboard
4	Security Management Server
5	Internal network

Figure 75. Typical deployment of a security gateway and a security management server (configurable using the SmartDashboard graphical user interface, or GUI).[96]

436. The Check Point R77 system was commercially available to purchase before the priority date of the '722 Patent. For example:

a. The CheckPoint Release Map shows that R77.20 was available for upgrade in July 2014. (Check_Point_R7x_xx_Releases_Maps_May_2017.pdf).

b. The splash screen on the Check Point R77.20 software indicates a copyright date "© 2014". (R77.20 Splash Screen).

c. A July 15, 2014 capture of the Check Point website indicates that "Check Point R77.20 is now available" and provides a link that customers can click to

[96] See pp. 9–10 CP_R77_Firewall_AdminGuide.

"Upgrade to R77.20 now." WayBack Machine July 15 2014 (https://web.archive.org/web/20140715095830/https:/supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doHome).

d. The Endpoint Security Administration Guide for CheckPoint R77.20 is dated November 10, 2014 and shows a revision history stating that the document was first released on July 22, 2014. (CP_R77.20_EndpointSecurity_AdminGuide).

e. On September 2, 2014, third party phoneboy.org reviewed CheckPoint R77.20. (http://phoneboy.org/2014/09/02/fun-with-check-point-dynamic-ip-gateways-in-r77-dot-20-with-gaia/).

437. For at least the reasons detailed below, it is my opinion that the Check Point R77 system enabled a person of ordinary skill in the art to practice each and every element of Claims 1 and 25 of the '722 Patent, and that said POSITA would be motivated to do so during the routine practicing of their typical duties. Thus, it is also my opinion that the Check Point R77 system anticipates these claims. In addition to the analysis presented herein, further discussion of relevant testing is described in Appendix E, which I incorporate by reference.

1. TEST CONFIGURATION WITH CHECK POINT R77

438. Exponent procured the Check Point R77 SMS product and installed it on a 32-bit PC-compatible Dell Latitude E6400 computer using the "Check_Point_R77.20_T124_Install.Gaia.iso" DVD ISO image.[97] Exponent also procured the Check Point R77 SG product and installed it on two 32-bit PC-compatible Dell PowerEdge 1750 computers using the "Check_Point_R77.20_T124_Install.Gaia.iso" DVD

[97] According to the Check Point website, DVD installation material was available in December 2010 (see https://supportcenter.Check Point.com/supportcenter/) and the installation procedure for the Firewall and Security Management Server is documented in the "R75 Installation and Upgrade Guide."

ISO image. The SMS and SGs were installed in a "Distributed Deployment" configuration (see Figure 75) wherein the SMS is installed on a different machine than the SGs.

439. Figure 76 shows the physical layout of the hardware used for Exponent's analysis, including the one security gateway, the security management server, the SmartDashboard (GUI), two switches, and two computers for sending and receiving packet traffic.

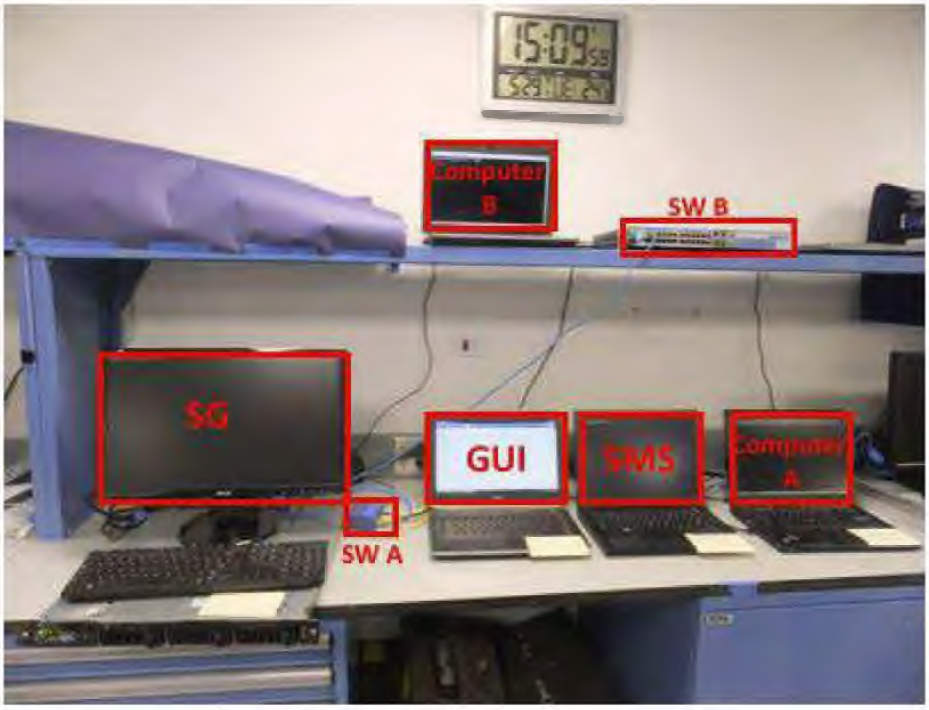


Figure 76. Photograph of test network used as part of the claim analysis that shows a hardware installation of one security gateway and one security management server with its associated SmartDashboard GUI. Computers A and B reside in two separate networks connected by the security gateway. Each network has one switch to route traffic.

440. Figure 77 shows the schematic layout of the test network used for Exponent's analysis. Network A includes the R77 SMS along with another computer, Computer A. Network B includes another computer called Computer B. Security Gateway 1, which includes a packet-filtering device, protects Network B from Network A.

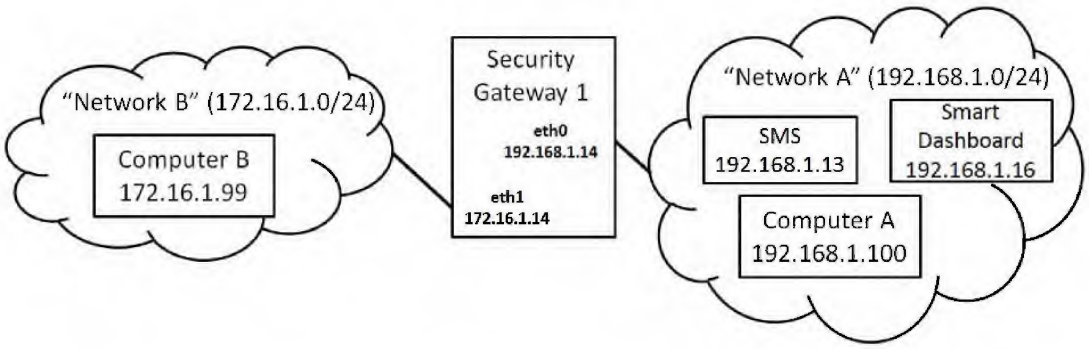


Figure 77. Schematic of test network architecture, including the static IP address of each element. Each network has its own subnet. SG 1 protects Network B from Network A. It has two Ethernet network interfaces (eth0 and eth1), which are used to pass traffic between networks.

441. The first subnet is called Network A and includes IP addresses in the range from 192.168.1.0 through 192.168.1.255. Network traffic internal to Network A is communicated via a TRENDnet TE100-S5 switch (Switch A).

442. The second subnet is called Network B and includes IP addresses in the range from 172.16.1.0 through 172.16.1.255. Network traffic internal to Network B is communicated via a VLAN on an HP ProCurve 2510-24 that uses the ProCurve Ethernet ports numbered 1–12 (Switch B).

2. CLAIM 1

443. **Claim 1a: A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

444. The Check Point R77 system is a network threat protection solution that includes the Check Point R77 Security Management Server (SMS) and one or more Check Point R77

Security Gateways (SGs). According to the Check Point R77 documentation,[98] the Security Management Server is "[t]he application that manages, stores, and distributes the Security Policy to the Security Gateways." A Security Gateway is "[a] computer or appliance that inspects traffic and enforces Security Policies for connected network resources," and the Security Policy is "[a] collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources through the use of packet inspection."(emphasis added). The method by which the Check Point R77 system provides network security involves filtering packets by applying a set of user-defined filters, and in doing so satisfies all requirements of claim element 1a of the '722 Patent.

445. I understand that the parties have agreed that the term "network-threat indicators" is to be construed as "indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like," and I have applied this claim construction throughout my analysis.

446. I also understand that there is a dispute regarding the construction of the term "packet-filtering device." More specifically, Plaintiffs have proposed that this term be construed as "a device programmed to filter packets based on data associated with a packet," while Defendants have proposed that no construction is needed and that this term should be given its "plain meaning." I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system comprises a "packet-filtering device," as explained below.

447. I also understand that there is a dispute regarding the construction of the term "packet-filtering rules." More specifically, Plaintiffs have proposed that this term be construed as

[98] See, generally, "CP_R77_SecurityManagement_AdminGuide.pdf" (dated 27 August 2013).

"condition or set of conditions that when satisfied cause a computing device to filter packets based on data associated with a packet," while Defendants have proposed "(i) packet-identifying criteria and (ii) an operator to be performed on the identified packets." I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 receives "a plurality of packet-filtering rules," as detailed below.

448. The Check Point R77 system is intended to be located at the interface between two different machines or networks, such that packets sent between said machines or networks must pass through the Check Point R77 Security Gateway. For example, in the test configuration described above, the Check Point R77 SG 1 is located between Computers A and B such that packets are not sent directly between these machines, but rather are first received by SG 1, which then in turn can pass the communication to its intended destination. More specifically: packets sent from Computer A to Computer B are received by the SG 1 via SW A, and then can be forwarded to Computer B via SW B; similarly, packets sent from Computer B to Computer A are received by the SG 1 via SW B, and then can be forwarded to Computer A via SW A. The Check Point R77 system does not have to forward all packets, however, and can instead perform a variety other functions, such as dropping, logging, rerouting, to packets that match certain criteria.

449. The criteria for identifying packets, and the functions that are performed on said packets, are determined using a set of filters that are configured by a user via the from the SmartDashboard GUI, associated with the Check Point R77 SMS, and communicated to the Check Point R77 SG. Each filter comprises at least one rule, which specifies at least one

criteria used to determine which packets are subject to the at least one rule, and at least one function that is to be performed on such packets.

450. Thus, at least because the Check Point R77 SG is programmed with rules, communicated by the Check Point R77 SMS, that filter packets according to criteria that may be based on data associated with the packet (such as IP addresses, URLs, packet data content, etc.) the Check Point R77 SG constitutes a "device programmed to filter packets based on data associated with a packet," which satisfies Plaintiff's proposed construction for "packet-filtering device." Also, in my opinion, a POSITA would recognize that the "plain meaning" for "packet-filtering device" is also satisfied by the Check Point R77 SG, at least because the Check Point R77 SG is a device that filters packets, and thus Defendants' proposed construction for "packet-filtering device" is also satisfied. Also, I note that each filter causes the Check Point R77 SG to filter packets based on data associated with each packet, at least because the Check Point R77 SG applies filters only to packets that match the applicable condition or conditions of the criteria of said filter: thus the filters satisfy Plaintiff's proposed construction for "packet-filtering rules." Similarly, at least because each filter comprises a criteria, which constitutes "packet-identifying criteria" and a function to be performed on matching packets, which constitutes "an operator to be performed on the identified packets," the filters satisfy Defendants' proposed construction for "packet-filtering rules."

451. Exponent has demonstrated on the Check Point R77 system test setup that user-defined packet-filtering rules can be sent to one or more packet-filtering devices, and then configured and deployed by creating "security policies" and installing those policies on selected security gateways.[99] The policies that are installed on the gateway may correspond to specific

[99] See, generally, "CP_R77_SecurityManagement_AdminGuide.pdf" (dated 27 August 2013) and "CP_R77_Firewall_AdminGuide.pdf" (dated 27 August 2013).

network threats.[100] A well-known example of a network-threat indicator is an uncommon request during normal web browsing. Because WebDAV HTTP methods are not commonly used in conventional web browsing, the use of methods such as the WebDAV method "MKCOL" is considered a network threat.

452. The SmartDashboard was used to install a policy that logs WebDAV HTTP methods. The policy can be configured either to allow offending packets to continue to their destination (by setting the policy action to "Detect") or to prevent offending packets from continuing to their destination (by setting the policy action to "Prevent") As a specific example, the WebDAV HTTP request "MKCOL / HTTP/1.0" attempts to create a new directory, which is an uncommon request during normal web browsing. A packet containing such a request can be flagged as corresponding to a network threat and the associated packets can be logged and blocked.

453. In Exponent's Check Point R77 system test setup, SG 1 serves as a packet-filtering device and can be configured to identify packets based on packet-filtering rules, as shown in Figure 78. This figure further shows that the Check Point R77 SG is not limited to receiving a single packet filtering rule, but can in fact receive a plurality of such rules corresponding to various network threats.

454. Specific HTTP method settings were configured, with the details shown in Figure 79, and the SG was installed in order to demonstrate that it can receive the packet-filtering rules, as shown in Figure 80 and Figure 81.

---

[100] See "CP_R77_Firewall_AdminGuide.pdf" (dated 27 August 2013) at Chapters 7 and 8.

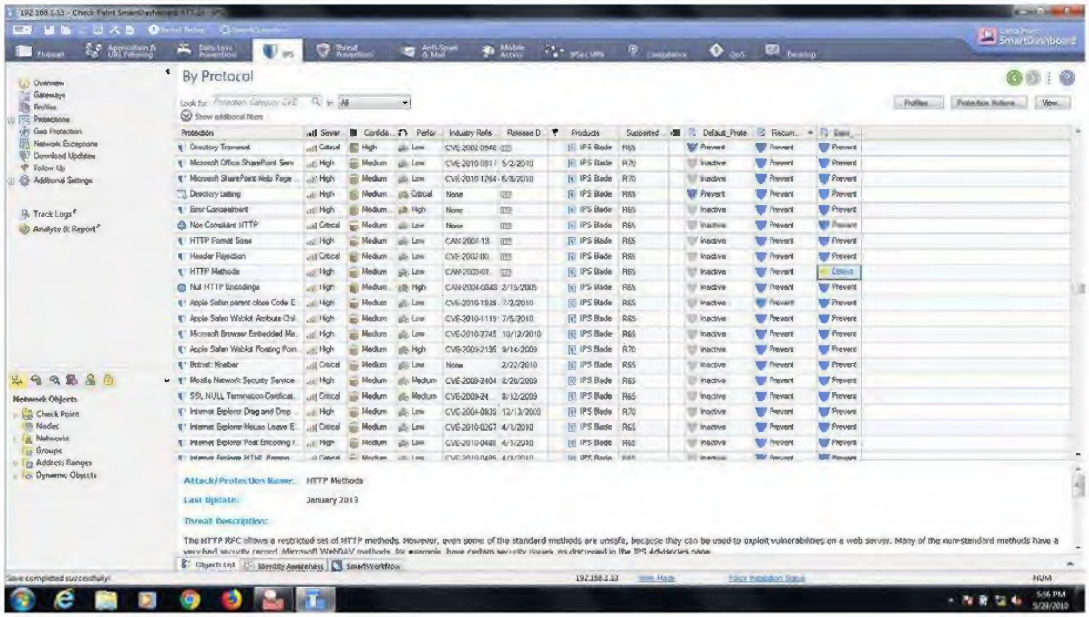


Figure 78. Screenshot of the SmartDashboard showing a plurality of packet-filtering rules that correspond to various network threats.

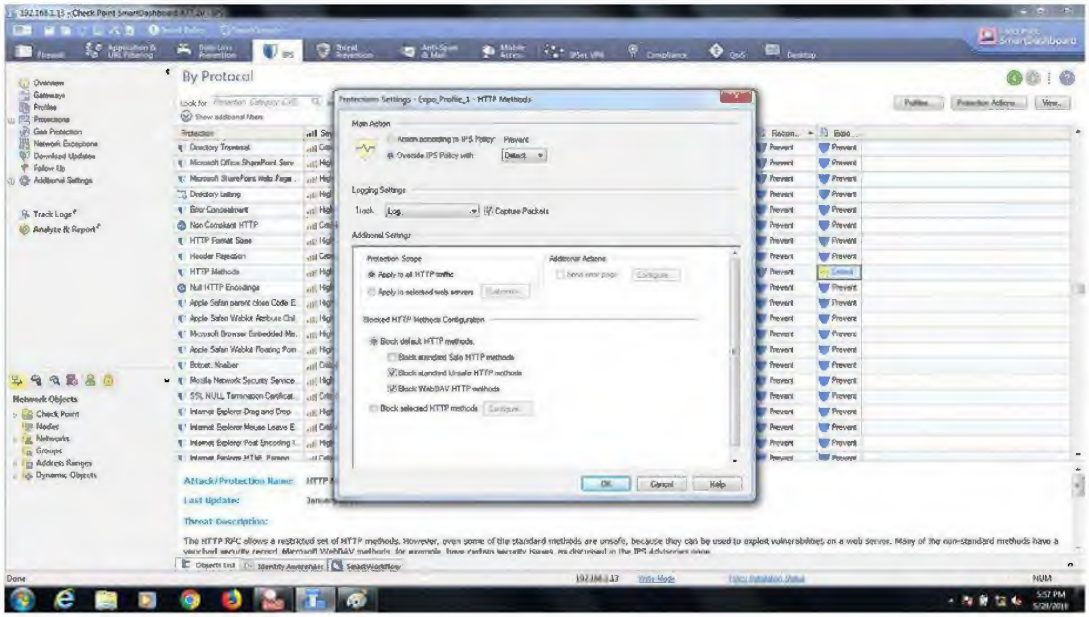


Figure 79. Screenshot of the SmartDashboard showing that the HTTP methods network threat is set to “Detect” mode for this policy.

CENTRIPETAL-CSCO 087674

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 174

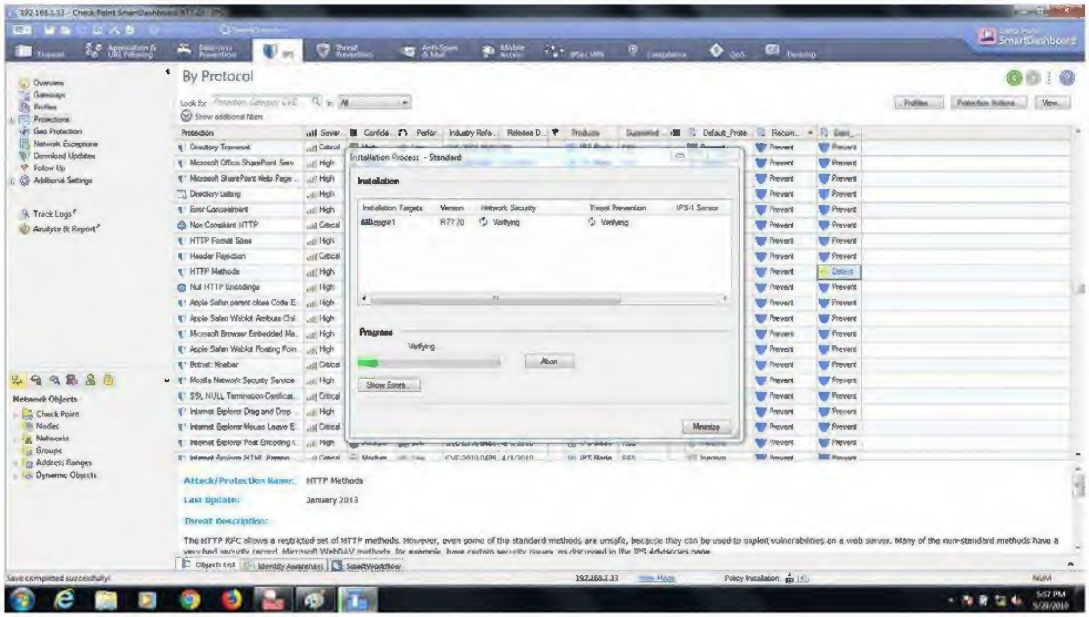


Figure 80. Screenshot of the SmartDashboard showing the installation of the policy.

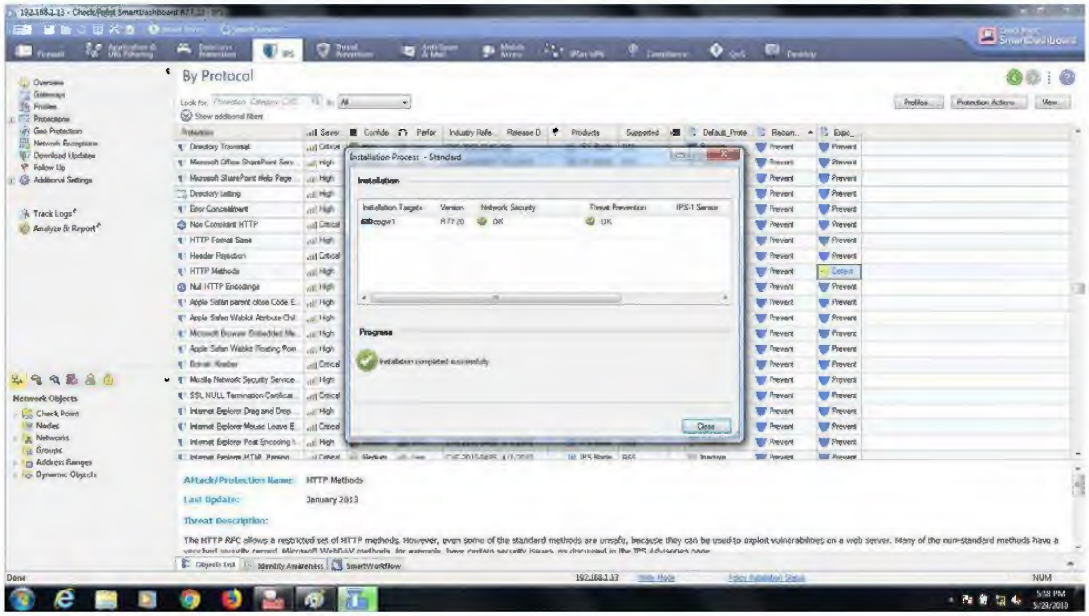


Figure 81. Screenshot of the SmartDashboard showing that the policy installation on the SG was successful.

CENTRIPETAL-CSCO 087675

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 175

455. Thus, Exponent has demonstrated that the Check Point R77 system operates a method in which the it receives "a plurality of packet-filtering rules configured to cause the packet filtering device [Check Point R77 SG] to identify packets corresponding to at least one of a plurality of network-threat indicators," as detailed below, and hence satisfies the requirements of this claim element.

456. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 1a of the '722 Patent.

457. **Claim 1b: receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

458. Check Point R77 includes a SmartLog program to log the action of the packets that are received by the SG. Figure 82 shows that the SG receives a plurality of packets, including a first packet, a second packet, and more. In this case, both the first packet and the second packet correspond to the HTTP methods network threat described above in relation to claim element 1a.

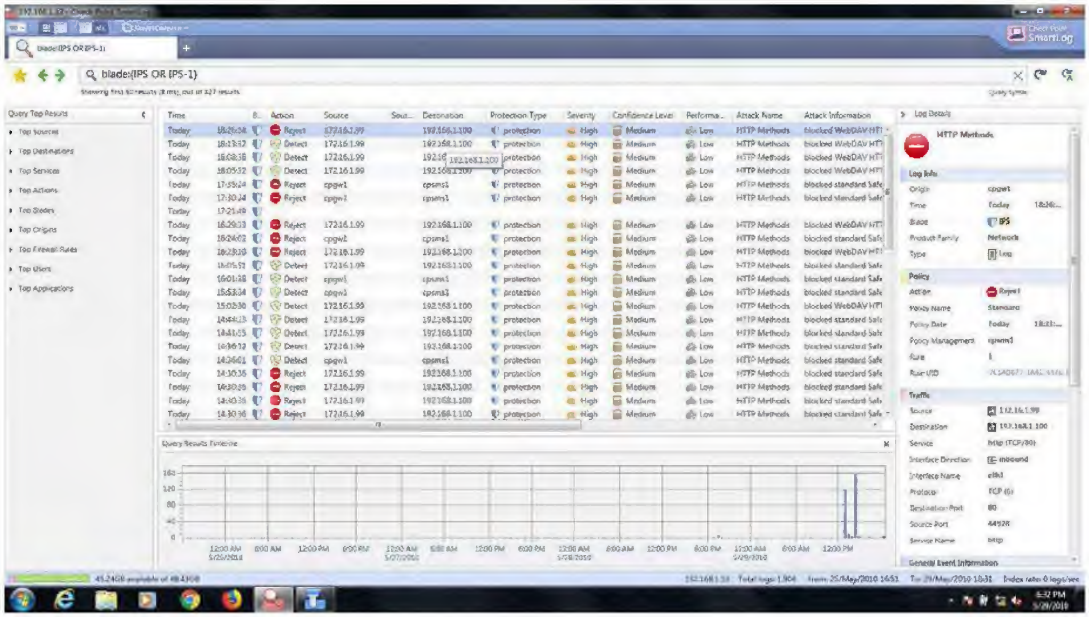


Figure 82. Screenshot of the SmartLog showing a plurality of packets having been received.

459. Thus, we have demonstrated receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet.

460. Thus, as demonstrated above, the Check Point R77 system performs a method that satisfies all requirements of claim element 17b of the '722 Patent.

461. Therefore, for at least the reasons above, it is my opinion that claim element 17b of the '722 is anticipated by the Check Point R77 system.

462. **Claim 1c: responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators: applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a**

CENTRIPETAL-CSCO 087677

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 177

destination of the first packet. As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

463. I understand that there is a dispute regarding the construction for "responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators." More specifically, Plaintiffs have proposed that this term be construed as "if the packet-filtering device determines the first packet meets one or more conditions associated with one or more network threat indicators from a packet filtering rule," while Defendants propose that no construction is needed and this term should be given its "plain meaning." I have considered both proposed construction in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system satisfies all requirements of claim element 1c, for at least the reasons below.

464. I also understand that there is a dispute regarding the construction of the term "operator." More specifically, Plaintiff has proposed that this term be construed as "an adjustable instruction that causes the packet filtering device to either prevent or allow a packet to continue to a destination," while Defendants have proposed that this term be construed as "function to either prevent a packet corresponding to criteria from continuing or allow it to continue to its destination." I have considered both proposed claim constructions in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system satisfies all requirements of claim element 1c, for at least the reasons below.

465. As described in detail in relation to claim elements 1a-b, Exponent has demonstrated the successful installation of a packet-filtering rule on the SG, corresponding to the HTTP methods network threat (which filters uncommon WebDAV HTTP requests), in conjunction with a "first packet" and a "second packet." Exponent has also demonstrated the execution of said packet-filtering rule, as discussed below and in relation to claim elements 1a-b.

466. An HTTP request (including a first packet) was sent from Computer B to Computer A. Figure 83 illustrates this request, which shows: (1) the initiation of a connection from Computer B to Computer A using the "netcat" utility (first line), (2) the HTTP request "MKCOL / HTTP/1.0" including the MKCOL method (second line), and (3) the response received from Computer A (remaining lines).

467. The response from Computer A is a 501 error code, indicating that the HTTP server[101] does not support the MKCOL method (along with some response headers and some HTML code indicating the error). This means that the packet sent from Computer B was allowed to pass through the packet filter to Computer A, which received the packet and sent back the error code. Additionally, Figure 84 shows the terminal session from HTTP server on Computer A. This figure displays the received MKCOL HTTP request on the fourth line.

[101] The HTTP server being used is the python SimpleHTTPServer module. For more information, see https://docs.python.org/2/library/simplehttpserver.html.

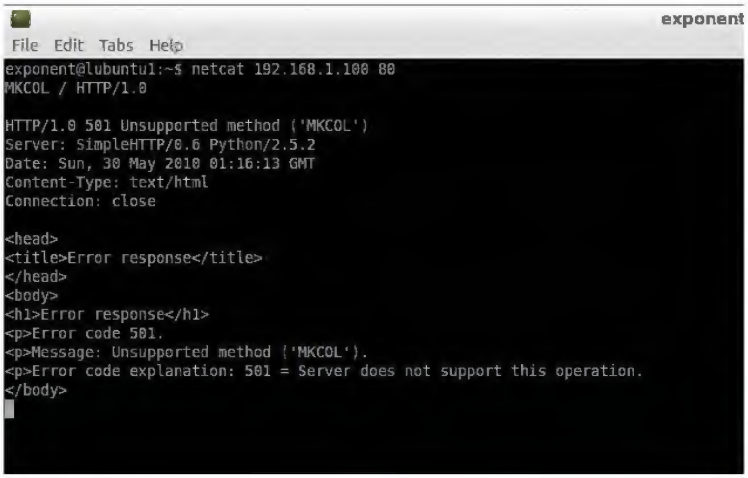


Figure 83. Screenshot of Computer B illustrating the successful send of the first packet.

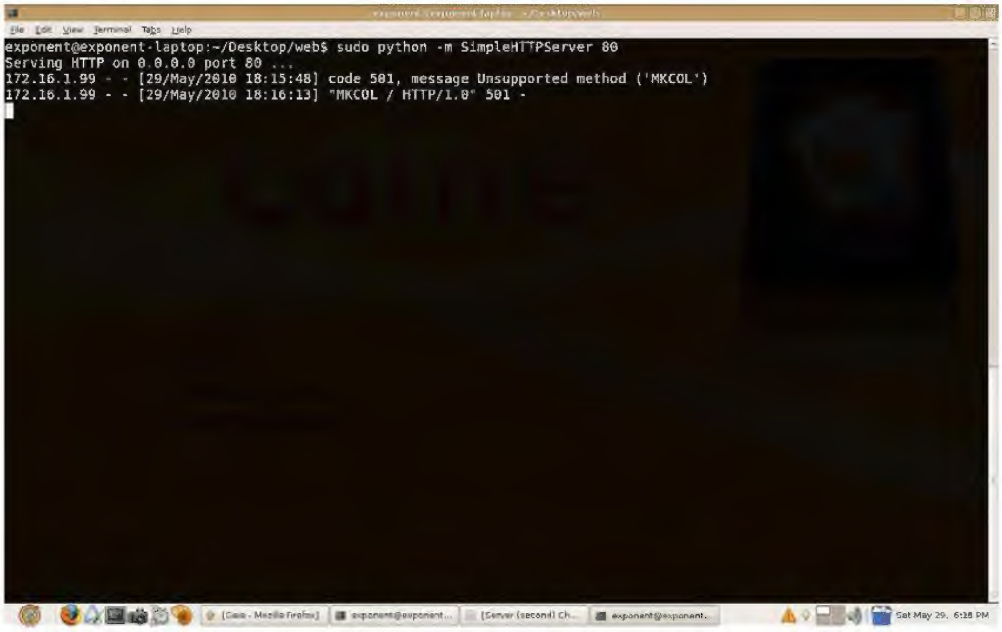


Figure 84. Screenshot of Computer A showing the successful receipt of the first packet

468. During the above-described demonstration, both the first packet and second packet constituted a "network threat indicator" and satisfied the criteria of the WebDAV HTTP methods filter. For the first packet, this filter was set to "Detect," which caused the filter to cause the Check Point R77 to allow the first packet to continue towards its destination, while

also creating a corresponding log entry in the SmartLog program, as shown in Figure 82. Thus, the first packet in the above-described demonstration, and its interaction with the Check Point R77 system, satisfies all requirements of claim element 1c.

469. More specifically, in view of Defendants proposed claim construction "if the packet-filtering device determines the first packet meets one or more conditions associated with one or more network threat indicators from a packet filtering rule," this proposed construction has been satisfied by the above-described demonstration at least because: (1) the HTTP methods filter is only applied if the Check Point R77 determines that the first packet meets the associated conditions, i.e. that said packet is attempting a WebDAV HTTP request; (2) the associated conditions correspond to a network threat indicator, at least because making such an HTTP request constitutes an uncommon request during normal web browsing

470. Also, the above-described demonstration satisfies both parties' proposed constructions for "operator": Regarding Plaintiff's construction, the "Action" performed upon packets that match the criteria of the HTTP Methods filter constitutes "an adjustable instruction that causes the packet filtering device to either prevent or allow a packet to continue to a destination" at least because the "Action" can be adjusted in the "Protection Settings" to either allow or prevent matching packets from continuing to their destination; regarding Defendant's construction, the "Action" constitutes a "function to either prevent a packet corresponding to criteria from continuing or allowing it to continue to its destination" at least because said "Action" can be set such that the filter either prevents or allows packets that correspond to the filter criteria to reach their destination.

471. Thus, the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1c.

472. Therefore, for at least the reasons above, it is my opinion that claim element 1c is anticipated by the Check Point R77 system.

473. **Claim 1d. communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

474. I understand that there is a dispute regarding the construction for the term "communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet." More specifically, Plaintiff has proposed that this term be construed as "causing a packet-filtering device to generate and communicate a record that identifies (1) a network threat indicator based on a rule and (2) data that indicates that the first packet was allows to continue toward the destination," while defendants have proposed that no construction is required and this term should be given its "plain meaning." I have considered both proposed claim constructions in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system satisfies all requirements of this claim, as detailed below.

475. The demonstration described above in relation to claim elements 1a-c demonstrates that the Check Point R77 system satisfies all requirements of claim element 1d. More specifically, the SmartLog program display presented in Figure 85 explicitly shows that the source of the first packet is 172.16.1.99 and the destination of the packet is 192.168.1.100,

and thus verifies that the packet-filtering device (the SG) communicates with the SMS that the first packet was allowed to pass.

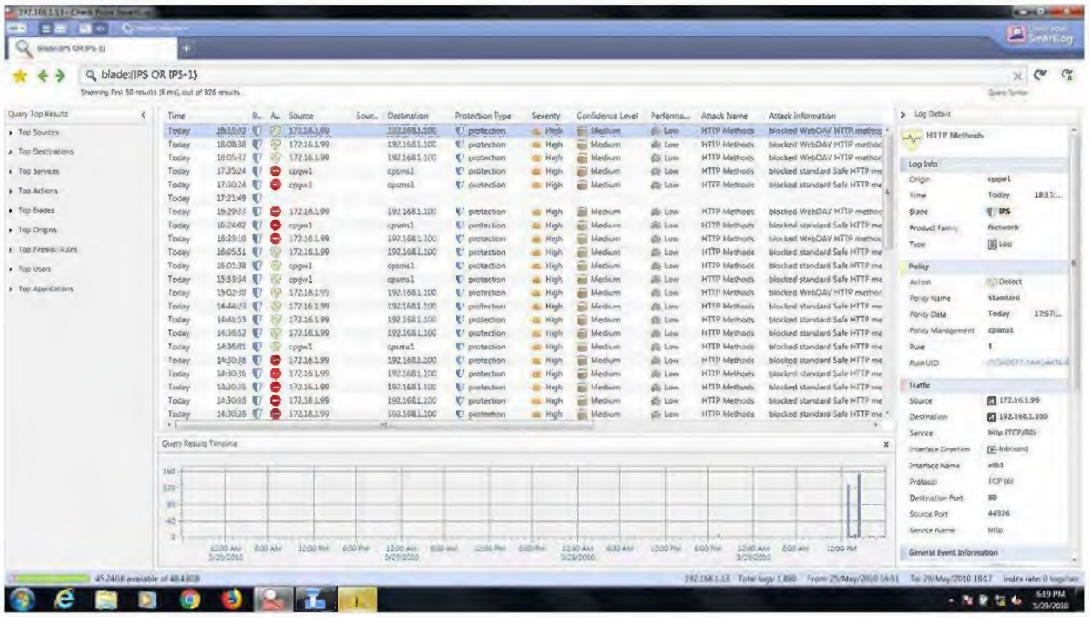


Figure 85. Screenshot of the SmartLog showing that the packets were allowed to move toward the destination.

476. The Check Point R77 SmartLog program[102] displays log files stored on the computer hosting the SMS. In order for the SmartLog program to display the information that the network attack packet corresponding to the HTTP methods threat was allowed, the SG must have communicated (to the SMS) data indicative that the packet was allowed. Therefore, this log constitutes the Check Point R77 communicating information from the HTTP methods filter that identifies which filter generated the log entry (and thus identifies the associated network-threat indicators that correspond to this filter). Thus, the plain meaning of the requirements of this claim, as would be understood by a POSITA, have been satisfied by the demonstration presented in relation to claim elements 1a-c.

---

102 See, generally, "CP_R77_SmartLog_AdminGuide.pdf" (dated 26 August 2013).

477. Plaintiff's proposed claim construction is also satisfied by the above-described demonstration, at least because the Check Point R77 SG 1, which constitutes a "packed-filtering device" has generated and communicated a record that: (1) includes the particular filter that caused the record to be generated, which contains the network threat indicator upon which said filter responds to; and (2) entries in the SmartLog program display that indicate both the source and destination of packets, including packets that were allowed to continue toward their destination.

478. Thus, for at least the reasons above, it the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1d.

479. Therefore, for at least the reasons above, it is my opinion that element 1d is anticipated by the Check Point R77 system.

480. **Claim 1e: causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

481. I understand that there is a dispute regarding the construction for "interface." More specifically, Plaintiff has proposed that this term be construed as "plain and ordinary meaning," while Defendants have proposed that this term be construed as "a display visible to the user that allows a user to provide input." I have considered both proposed constructions in my analysis, and I reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system satisfies all requirements of claim element 1e, as detailed below.

482. x

483. As described above in relation to claim element 1d, the SmartLog shown in Figure 85 satisfies the requirements of claim element 1e. Figure 86 also shows a GUI that displays information about the details of the packet-filtering rule for the HTTP methods network threat, and thus also satisfies the requirements of claim element 1e. More specifically, the SmartLog forms part of the system interface and displays information corresponding to the packet-filtering rules, such as the filter used for the above-described demonstration. The SmartLog is displayed on the Check Point R77 SmartDashboard GUI, that was viewed during testing via the screen on a laptop (see Figure 76). The Check Point R77 SmartDashboard GUI enables a user to interact with the Check Point R77 system, e.g. view and amend settings, view logs, etc., and thus satisfies the plain and ordinary meaning for the term "interface" as would be understood by a POSITA. Also, the Check Point R77 SmartDashboard GUI constitutes "a display visible to the user that allows a user to provide input," as least because a user is able to see said GUI and use it to alter the filter settings as demonstrated above in relation to claim elements 1a-c. Therefore, both Plaintiff's and Defendants' proposed constructions for "interface" are satisfied by the Check Point R77 SmartDashboard GUI.

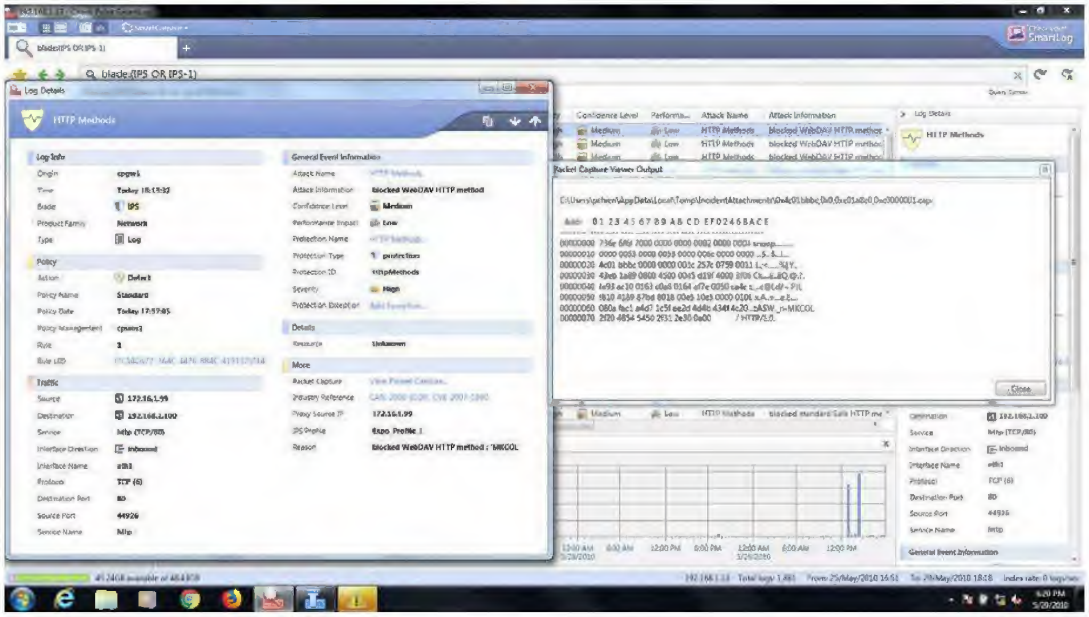


Figure 86. Screenshot of the SmartLog showing the details of the packets allowed to move toward the destination.

484. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1e.

485. Therefore, for at least the reasons above, it is my opinion that claim element is anticipated by the Check Point R77 system.

486. **Claim 1f: receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

487. I understand there is a dispute regarding the construction of the term "user." More specifically, Plaintiff has proposed that this term be given its "plain and ordinary meaning," while defendants have proposed that this term be construed as "person (e.g., administrator)."

I have considered both claim constructions in my analysis, and reserve the right to modify my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system satisfies all requirements of this claim. In any event, it is my opinion that the plain and ordinary meaning of the term "user" includes "person (e.g., administrator).

488. As described in relation to claim elements 1a-c, the Check Point R77 SG 1 constitutes a packet-filtering device, and has been demonstrated to receive instructions generated in response to a user, such as a person, invoking a selection within a menu of settings for the HTTP methods filter: this settings window is shown, for example, in Figure 79, in which the "Protections Settings" menu that comprises "an element in the at least one portion of the interface" is shown. As detailed in relation to elements 1a-c, this menu allows for the determination of an "Action," which corresponds to the function, or "Policy Mode," that will be performed by the HTTP methods filter upon packets that match the associated network-threat indicator.

489. The HTTP methods network attack settings in the demonstration above were initially configured to detect the attack, as Figure 78 shows, but not block it. After the first packet was logged (detected), the user reconfigured the HTTP methods attack settings from "Detect" to "Prevent" by clicking the GUI near the highlighted section of Figure 87. The updated policy was then installed on the security gateway. The updated settings are also shown in Figure 88.

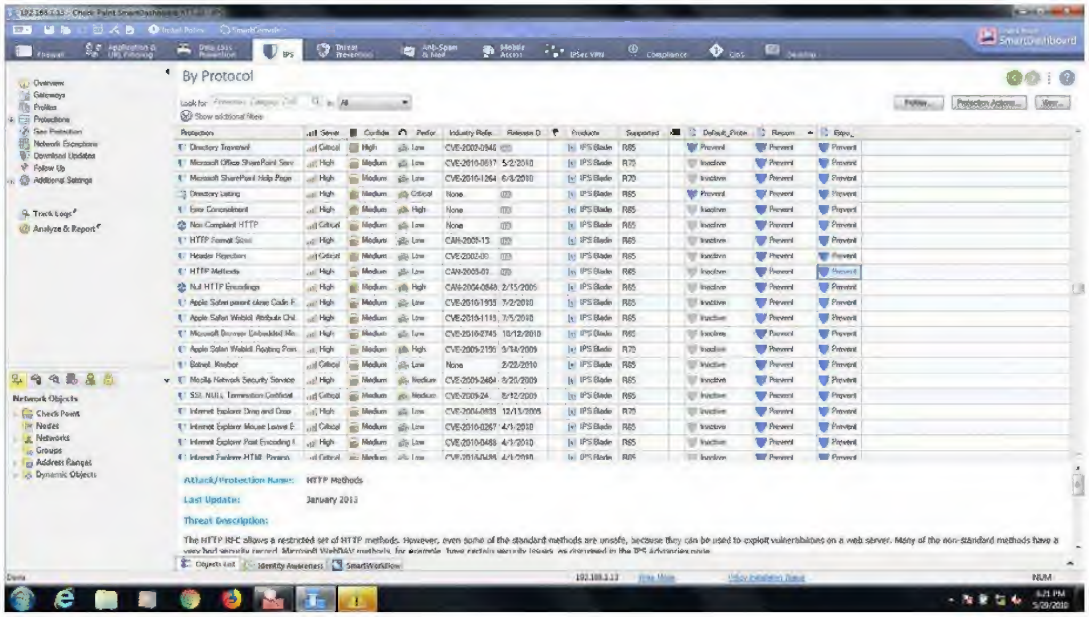


Figure 87. Screenshot of SmartDashboard showing the HTTP methods policy in "Prevent" mode. This change was in response to user action.

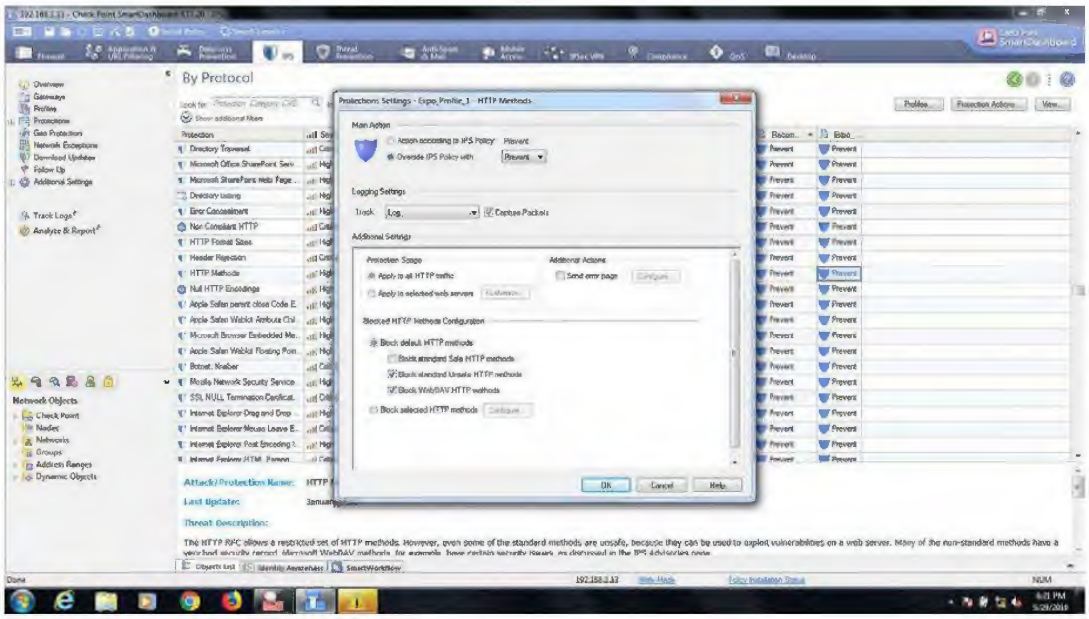


Figure 88. Screenshot of SmartDashboard showing detailed information of the HTTP methods policy after changing the policy to "Prevent."

490. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1f.

491. Therefore, for at least the reasons above, it is my opinion that claim element 1f is anticipated by the Check Point R77 system.

492. **Claim 1g: responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

493. I understand that there is a dispute regarding the construction of the term "modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their destination." More specifically, Plaintiff has proposed that this term be construed as "modifying the state of the packet-filtering device to cause an adjustable instruction to prevent a packet from continuing toward its destination," while Defendants propose that no construction is required and this term should be given its "plain meaning." I have considered both proposed constructions in my analysis, and I reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system satisfies all requirements of claim element 1g, as detailed below.

494. Figure 89 and Figure 90 show that the packet-filtering rule corresponding to the HTTP methods network attack was installed on the SG. As demonstrated above in relation to claim elements 1a-c, it was shown that the Check Point R77 system allowed a first packet that

corresponded to the criteria of the HTTP methods filter to be permitted to reach its final destination when the "Action" setting for said filter was set to "Detect"; however, as shown in relation to claim element 1f, the "Action" setting was subsequently changed using the Check Point R77 SMS GUI to "Prevent." This demonstrated that the operator performed by the HTTP methods filter was modified in response to the Check Point R77 SG receiving an instruction from the Check Point R77 SMS GUI (SmartDashboard). Thus, the SG was reconfigured to block packets containing WebDAV HTTP methods from continuing toward their respective destinations. Therefore, the "plain meaning" of this claim element, as would be understood by a POSITA, has been demonstrated as being satisfied by the Check Point R77 system.

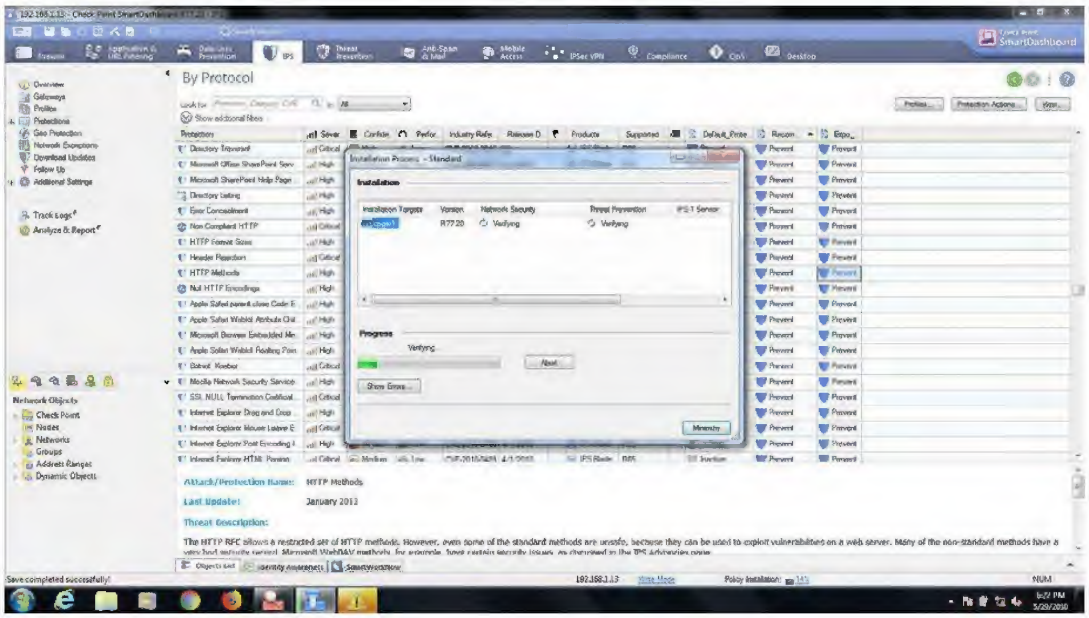


Figure 89. Screenshot of SmartDashboard showing the installation of policies on the SG.

CENTRIPETAL-CSCO 087690

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 190

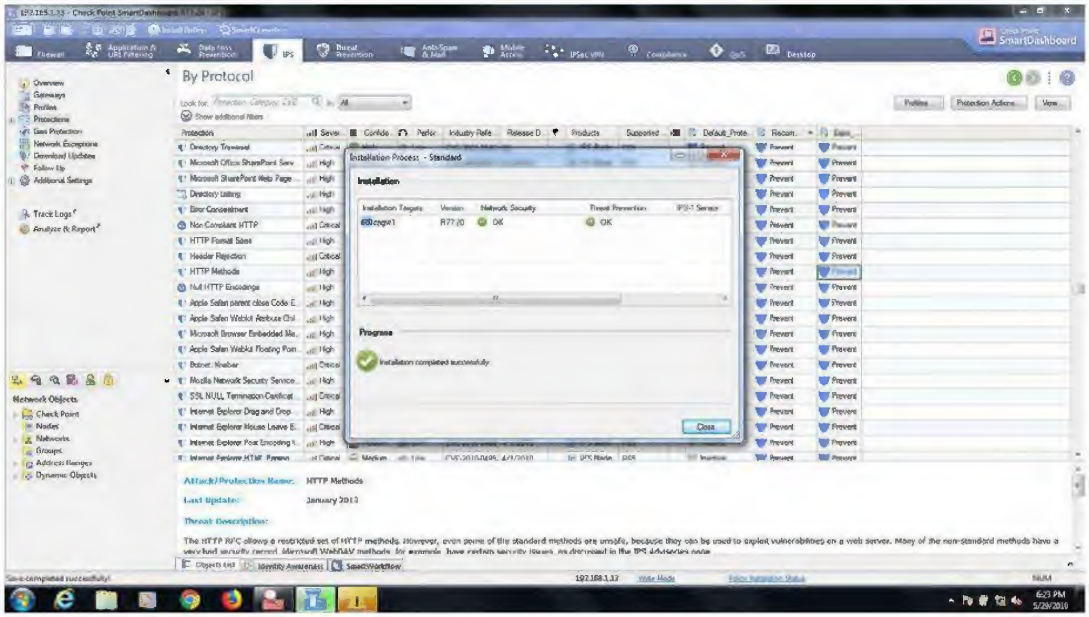


Figure 90. Screenshot of SmartDashboard showing successful installation of the HTTP methods policy in "Prevent" mod.

495. Plaintiff's proposed claim construction of relevance to this claim element is also satisfied by the above-described demonstration. More specifically, the "Action" associated with the HTTP methods filter constitutes "an adjustable instruction" and setting this to "Prevent" constitutes "modifying the state of the packet-filtering device to cause an adjustable instruction to prevent a packet from continuing toward its destination."

496. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1g.

497. Therefore, for at least the reasons above, it is my opinion that claim element 1g is anticipated by the Check Point R77 system.

498. **Claim 1h: responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria: preventing by the packet-filtering device, the second packet from continuing toward a destination of the second**

packet; As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

499. As described above, Exponent has shown that a security policy containing a packet-filtering rule corresponding to the HTTP methods threat was previously installed on the Check Point R77 SG. As demonstrated above, in relation to claim element 1g, the user-modified "Action" was changed to "Prevent" such that the "Security Policy" of the SG was reconfigured to block packets containing WebDAV HTTP methods from continuing toward their respective destinations.

500. A WebDAV HTTP request including the second packet was sent from Computer B to Computer A. Figure 91 exhibits this action and shows: (1) the initiation of a connection from Computer B to Computer A using the netcat utility (first line), (2) the HTTP request "MKCOL / HTTP/1.0" including the MKCOL method (second line), and (3) the lack of a response (no subsequent lines of the netcat session).

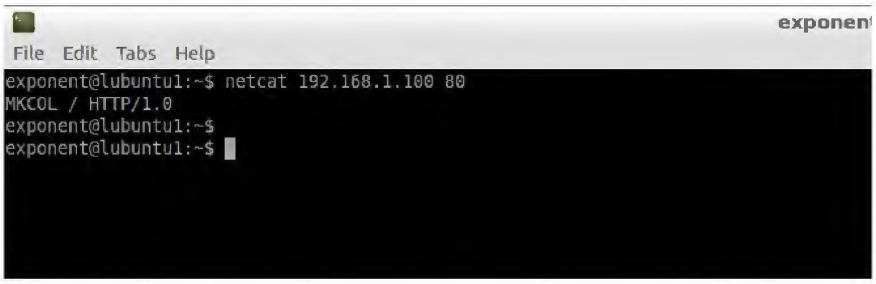


Figure 91. Screenshot of Computer B unsuccessfully sending WebDAV request to computer A.

501. The Check Point R77 determined the second packet matched the criteria of the HTTP methods filter as confirmed via inspection of the SmartLog, which included an entry corresponding to the determination that the criteria of the HTTP methods filter were satisfied.

502. That the second packet was prevented from continuing toward its destination was confirmed by the fact that Computer A never received the HTTP request from Computer B, and Computer B did not receive a response to the packet it tried to send. Had Computer A received the HTTP request, it would have sent back a response, including a 501 error code. Thus, the second packet was prevented from continuing toward its destination. Furthermore, Figure 92, which depicts the terminal session from the HTTP server running on Computer A, shows that the server did not receive a MKCOL request.[103]

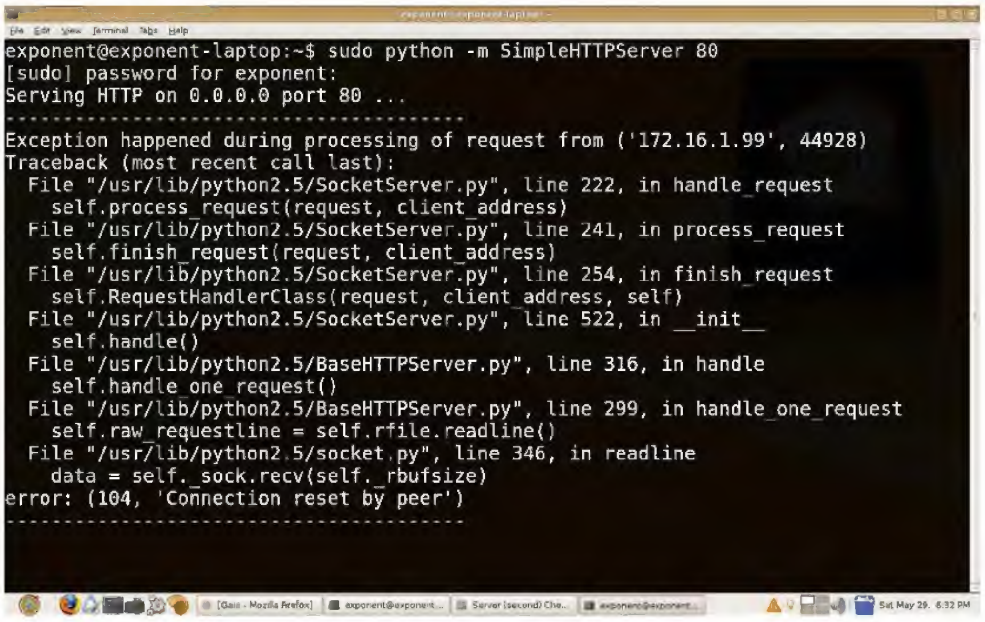


Figure 92. Screenshot of Computer A showing that the packet-filtering device prevented the WebDAV request from Computer B.

503. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1h.

504. Therefore, for at least the reasons above, it is my opinion that claim element 1h is anticipated by the Check Point R77 system.

---

[103] Rather, the connection was dropped leading to the cascade of exceptions shown in the lower half of the figure.

CENTRIPETAL-CSCO 087693

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 193

505. **Claim 1i: communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

506. The SmartLog shows data indicative that the second packet was prevented from moving toward its intended destination. As exhibited in Figure 93, the SmartLog indicates that the HTTP method network threat was rejected by the packet-filtering device and was thereby prevented from continuing toward its intended destination. In addition to blocking the second packet, the Check Point R77 SG 1 also communicated data that the second packet was blocked. This is known because in order for the Check Point R77 SmartLog program to display the information that the network attack packet corresponding to the HTTP methods threat was blocked, the SG must have communicated such data to the Check Point R77 SMS.

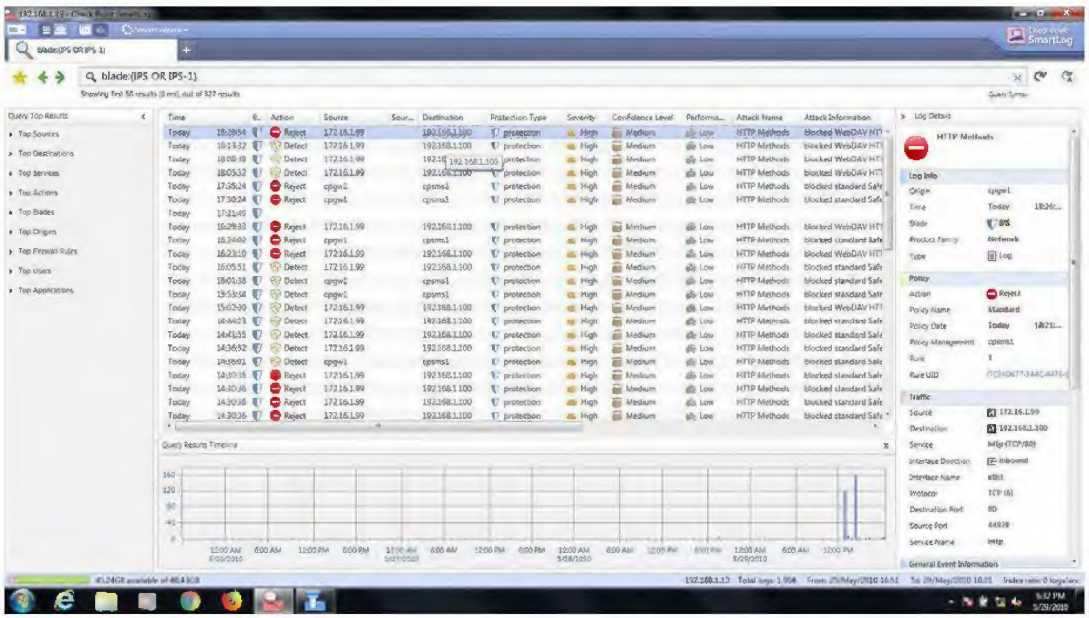


Figure 93. Screenshot of the SmartLog showing that packets were prevented from moving toward the destination.

CENTRIPETAL-CSCO 087694

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 194

507. Thus, at least for the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1i.

508. Therefore, for at least the reasons above, it is my opinion that claim element 1i is anticipated by the Check Point R77 system.

509. **Claim 1j: causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

510. That the packet-filtering device prevented the second packet from continuing on to its destination was demonstrated in relation to claim element 1h, and evidence that the packet-filtering device had communicated such information was demonstrated in relation to claim element 1i.

511. The SmartLog display, shown in Figure 94, displays information about the details of the packet-filtering rule for the HTTP methods network threat, including information indicating that the second packet was prevented from moving toward its intended destination.. For at least these reasons, the SmartLog display constitutes an interface that includes "display of the data indicative that the second packet was prevented from continuing towards" its destination.

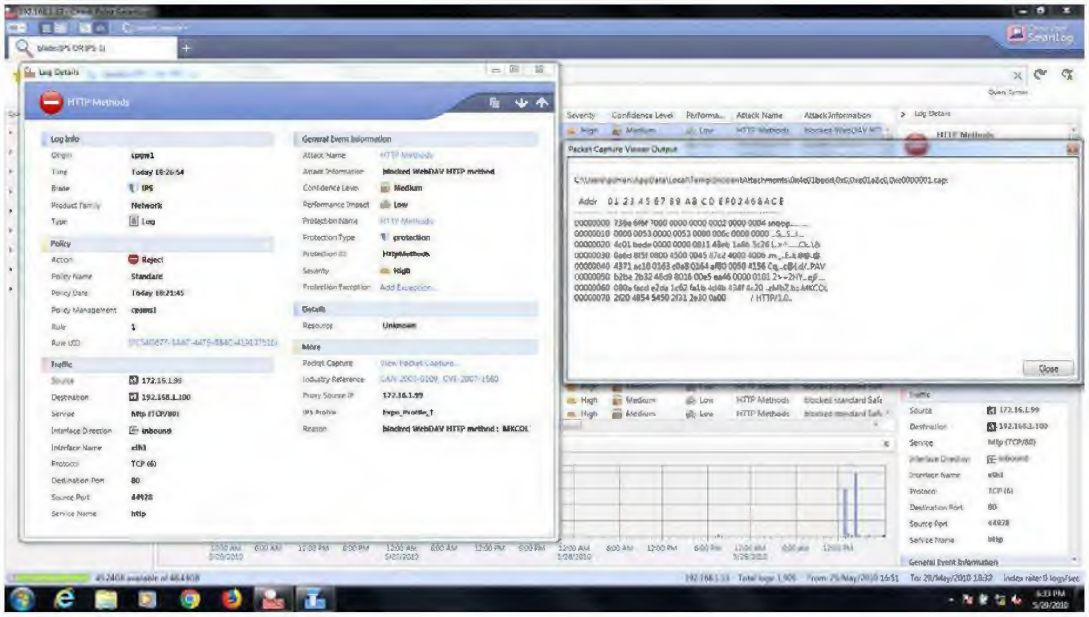


Figure 94. Screenshot of the SmartLog showing details of the packets prevented from moving toward the destination.

512. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirements of claim element 1j.

513. Therefore, at least for the reasons above, it is my opinion that claim element 1j is anticipated by the Check Point R77 system.

514. For at least the reasons detailed above, it is my opinion that the Check Point R77 system satisfies each and every limitation of claim 1 of the '722 Patent. Consequently, for at least the reasons above, it is my opinion that claim 1 of the '722 Patent is anticipated by the Check Point R77 system.

3. CLAIM 25

515. **Claim 25: The method of Claim 1, wherein: receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different**

packet-filtering devices. This claim is dependent upon claim 1 of the '722 Patent, and as detailed above it is my opinion that claim 1 is anticipated by the Check Point R77 system. As detailed below, the Check Point R77 system also satisfies all limitations added to claim 1 of the '722 Patent by claim 25 therein.

516. As detailed in relation to claim 1a, each Check Point R77 SG constitutes a "packet-filtering device" as required by claim 25 and the relevant claim constructions; and, also as detailed in relation to claim 1a, the filters used by the Check Point R77 system constitute "packet-filtering rules" as required by claim 25 and the relevant claim constructions.

517. Although only one Check Point R77 SG was required for demonstrating that the Check Point R77 system satisfies the method of claim 1, the limitations added by claim 25 require use of more than one packet-filtering device. This was achieved by extending the test configuration described in Section XI,D,1 to include a second security gateway.

518. Figure 95 shows the physical hardware used to demonstrate that the Check Point R77 system satisfies all requirements added to claim 1 by claim 25, and Figure 96 shows the corresponding network map for the extended test network that includes two different security gateways (SG1 and SG2)

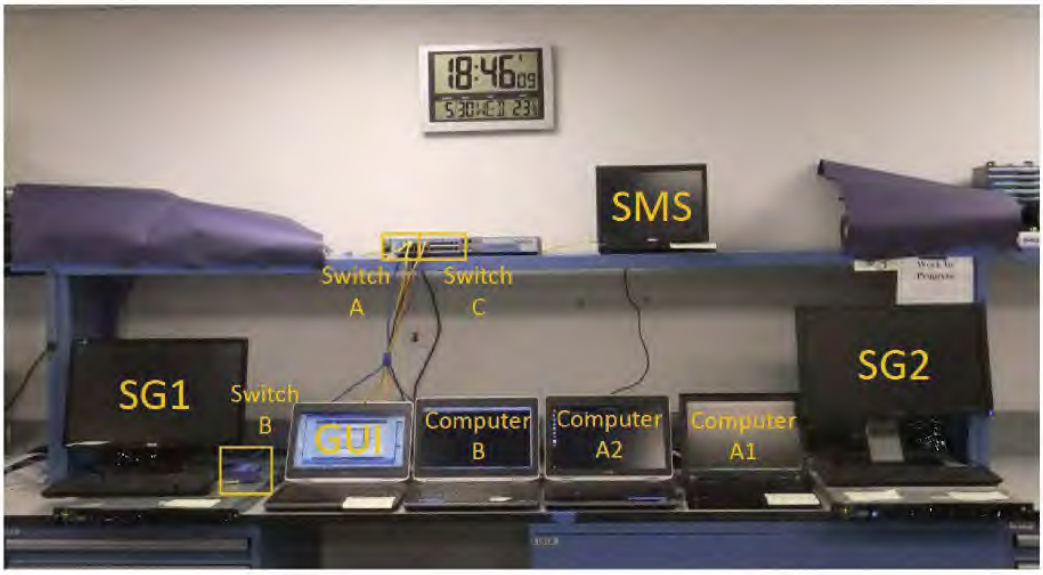


Figure 95. Annotated photograph of the test network used as part of this and subsequent claim analyses. The figure shows a hardware installation including two security gateways (SG1 and SG2) and one security management server (SMS) with its associated SmartDashboard GUI. Computers A1 and A2 reside in Network A. Computer B resides in Network B. Networks A and B are connected by SG1.

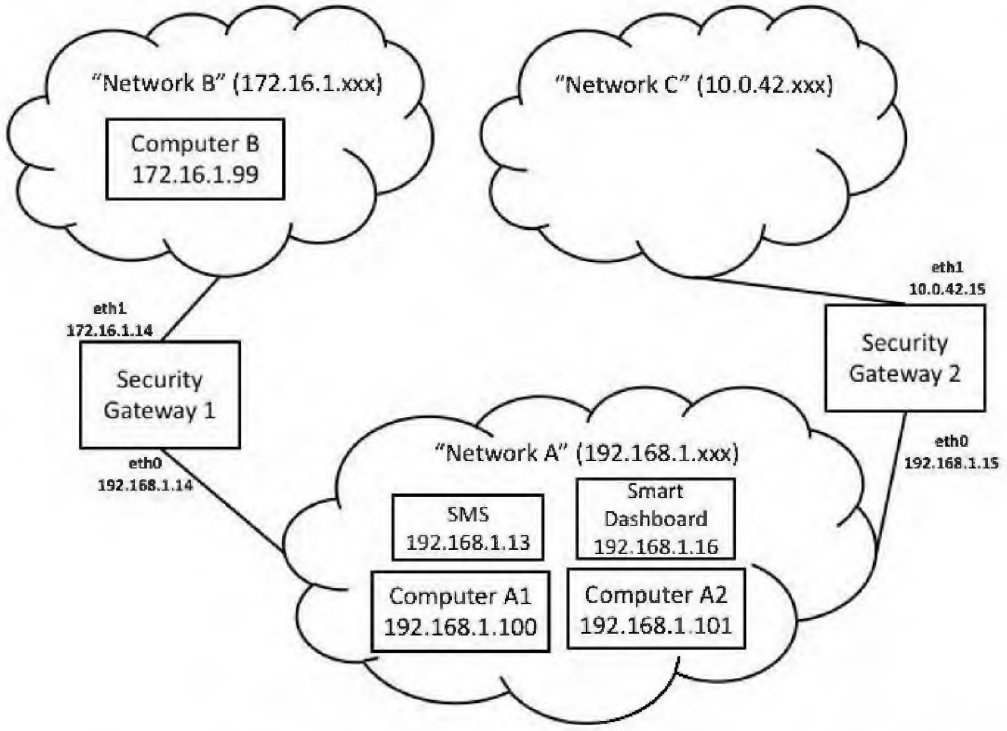


Figure 96. Schematic of test network architecture, including the static IP address of each element. Each network has its own subnet. Security Gateway 1 protects Network B from Network A. Security Gateway 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (eth0 and eth1), which are used to pass traffic between networks.

519. The packet-filtering device (SG 1) is connected to two networks via two separate Ethernet ports. The device is connected to Network A via Switch A and is connected to Network B via Switch B, as Figure 95 shows. Figure 95 also shows a second packet-filtering device (SG 2). The first subnet is called Network A and includes IP addresses in the range from 192.168.1.0 through 192.168.1.255. Network traffic internal to Network A is communicated via a VLAN on an HP ProCurve 2510-24 that uses the ProCurve Ethernet ports 1–12 (Switch A). The second subnet is called Network B and includes IP addresses in the range from 172.16.1.0 through 172.16.1.255. Network traffic internal to Network B is communicated via a TRENDnet TE100-S5 switch (Switch B). The third subnet is called

Network C and includes IP addresses in the range from 10.0.42.0 through 10.0.42.255. Network traffic internal to Network C is communicated via a VLAN on a HP ProCurve 2510-24 that uses the ProCurve Ethernet ports 13–24 (Switch C). For the analysis of this claim, Network B is taken as the first network and Network A is taken as the second network. For the analysis of this claim, the first host in the second network is taken to be Computer A2 and the second host in the second network is taken to be Computer A1.

520. Both Check Point R77 SG1 and SG2 can be independently configured via the Check Point R77 SMS GUI. The Check Point R77 SMS running on the laptop connected to the Check Point R77 system constitutes "one or more computing devices" that, in the same way as demonstrated in relation to claim 1 for Check Point R77 SG1, can "provide packet-filtering rules" to both Check Point R77 SG1 and Check Point R77 SG2.

521. As shown in Figure 97, multiple policies were installed via the computer running SmartDashboard on multiple packet-filtering devices (Security Gateway 1 "cpgw1" and Security Gateway 2 "cpgw2"). These policies contain multiple different packet-filtering rules. Consequently, the "one or more computing devices" can "provide packet-filtering rules to a plurality of different packet-filtering devices, which satisfies the limitations added to claim 1 by claim 25.

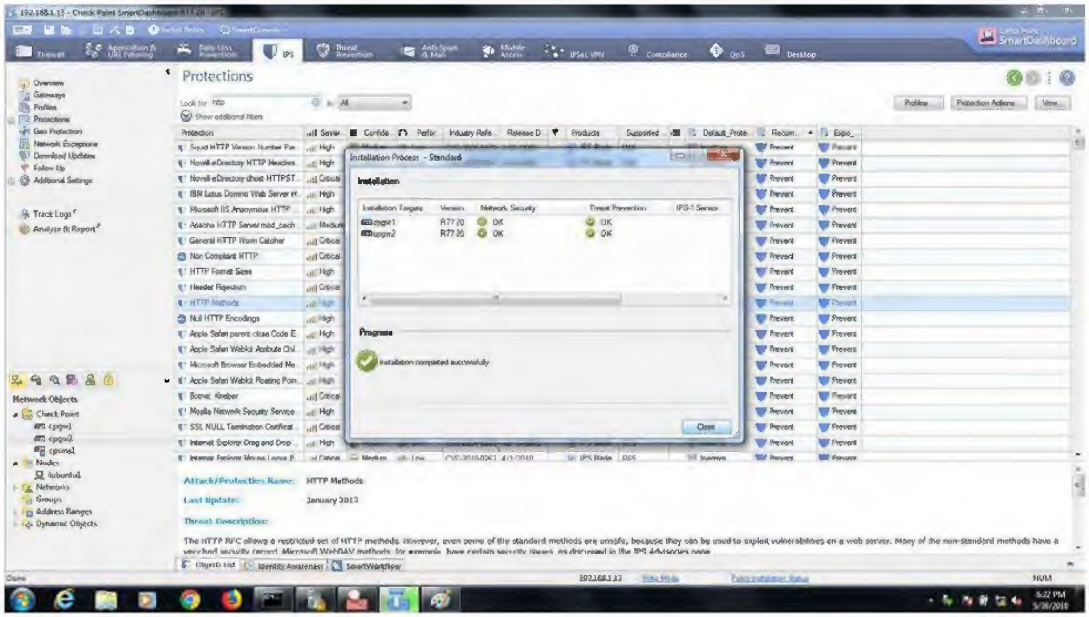


Figure 97. Screenshot of the SmartDashboard indicating the successful installation of policies on different packet-filtering devices.

522. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirement of claim 1 of the '722 Patent as well as all requirements added to this claim by claim 25 therein.

523. Therefore, at least for the reasons above, it is my opinion that the Check Point R77 system anticipates claim 25 of the '722 Patent.

E. OBVIOUSNESS IN VIEW OF US PATENT NO. 8,955,128 IN COMBINATION WITH POLIWALL AND NTO 7300

1. US PATENT NO. 8,955,128

524. US Patent No. 8,955,128 ("the '128 Patent"), entitled "Systems and Methods for Selectively Regulating Network Traffic," was filed on July 27, 2012, and I am informed by counsel that the '128 Patent constitutes prior art for the '722 Patent.

525. The '128 Patent is directed towards "systems and methods for controlling traffic to a network. More particularly, the invention is directed to systems and methods for regulating network traffic based on user preferences" (the '128 Patent, 1:15-18).

526. The invention of the '128 Patent seeks to "provide a method for reducing unwanted network traffic via easily configured lists" (the '128 Patent, 2:55-57), where "lists" are files that contain IP addresses (*see* the '128 Patent, 4:8-14) that are used to identify packets to which filtering rules should be applied. An objective of the '128 Patent is to allow filtering of packets based on country of origin, such that filters may be created to exclude all packets from pre-determined countries, or allow only packets from pre-determined countries. The invention of the '128 Patent contemplates the use of repositories that contain many lists, which may be updated from a "centralized server," stating:

> In an embodiment, the repository may be organized or compiled into any one or more of the following lists: Prebuilt Country IP lists, Subscribed Lists, Custom Lists, or Control Lists. The Prebuilt Contry IP Lists may be a pre-made list for each country. There files/lists may be updated from the centralized server 30 as information is obtained from the appliance 20. Subscribed Lists may include prebuilt lists which a user may choose to add or filter with. … Custom Lists are lists that the user can create based on their own criteria … Other lists which are not based on geographical boundaries may also be utilized. (the '128 Patent, 4:18-35)

527. Packets are filtered by a "rules engine" which uses "predefined rules to evaluate incoming information based on one or more predefined rules … determined by a user's preferences" (the '128 Patent, 3:42-46), and "[t]he desired lists … may be selected or turned on by the user through the user interface" (the '128 Patent, 4:36-37).

528. The '128 Patent discloses that the filtering device may be "located at any number of locations so long as it sits in between the Internet and the network it is designed to protect"

(the '128 Patent, 4:43-45). The appliance may also be a network transparent "Layer 2 network bridge" (the '128 Patent, 4:45-48). The use of packet-by-packet application of filtering rules upon packets that match criteria is also disclosed:

> In operation, when network traffic, such as individual packets, attempt to enter a network protected by the system of the invention, rules are applied, they are loaded into the network filter of the system in various chains as appreciated by one skilled in the art. As used herein, a "chain" refers to a series of rules that are applied to the incoming packets such that they can be handled in a pre-defined and automated way depending on whether or not they satisfy certain criteria or have certain characteristics (the '128 Patent, 4:49-57, emphasis added).

529. The invention of the '128 Patent may perform one or more actions to packets which satisfy the criteria of one or more rules. These actions can include: forwarding packets to the intended destination (*see* the '128 Patent, e.g. 4:61-67); dropping packets (*see* the '128 Patent, e.g. 5:1-24); logging packets (*see* the '128 Patent, e.g. 6:37-40).

530. The system disclosed by the '128 Patent also features a graphical user interface, which in addition to enabling the user to customize and select lists, and associated rules, also "display[s] real-time statistics" relating to network traffic, and enables the user to access various logs, alerts, and notifications (*see* the '128 Patent, e.g. 8:36-48; *see* the '128 Patent, Fig. 3).

2. POLIWALL

531. The TechGuard PoliWall packet filtering device ("PoliWall") has been available since at least 2006[104], and I am informed by counsel that PoliWall constitutes prior art for the '722 Patent.

[104] July 26, 2018 Deposition Transcript of David Masteas, CTO of Bandura, a wholly-owned subsidiary of TechGuard. See also discussion of Poliwall above.

532. PoliWall was advertised as "a high performance security appliance to thwart global network threats and analyze cyber attacks." This is achieved by placing PoliWall between a router (which may be connected to the Internet) and a network firewall, as depicted below in section of the PoliWall brochure.

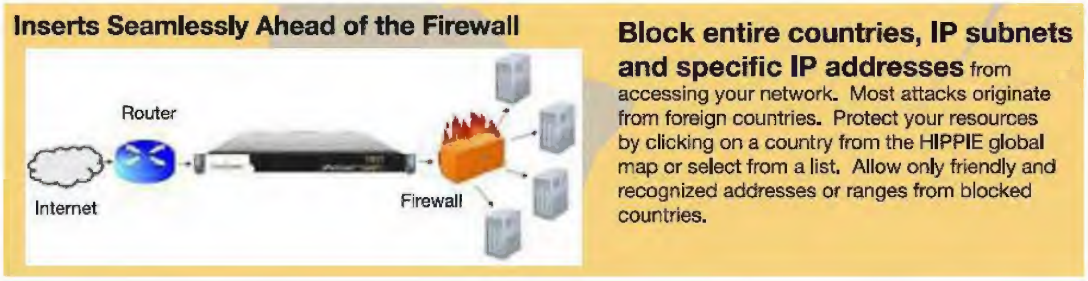


Figure 98 Excerpt from PoliWall brochure

533. PoliWall used its High-speed Internet Protocol Packet Inspection Engine ("HIPPIE") to enable rules to be applied to packets based upon their IP address of origin. This enabled users to set rules based upon geographical locations such that traffic from particular countries may be restricted. In addition to allowing all traffic from a particular country to be blocked, PoliWall also enabled a user to configure rules to enable all traffic from particular countries to be trusted and thus forwarded without restriction. Examples of restricting and allowing all traffic from particular countries is shown in a YouTube video[105] published on March 3, 2011, which counsel informs me constitutes a prior art reference for the '722 Patent.

3. NTO 7300

534. The Ixia Network Tool Optimizer™ NTO 7300 ("NTO 7300") is a network packet broker system for aggregating, filtering, and directing network data to tools such as data recorders, VoIP monitors, or other applications. This system includes line cards with ingress and egress ports and supervisor modules, which route traffic between the ports. A typical

[105] https://www.youtube.com/watch?v=z62og8lNk5A

usage case for the system is in a large network where traffic must be routed to many individual tools. The NTO 7300 can filter packets to reduce the load on the tools and balance the packet load among groups of tools.

535. The NTO 7300 system was commercially available to purchase prior to the priority date of the '722 Patent.

536. NTO 7300 is a "chassis-based high port density NTO platform" (*see* PA0013241). The NTO 7300 assists in network optimization by enabling network traffic to be filtered and directed to the appropriate device. For example, "[t]he NTO 7300 directs network data from SPAN ports and TAPS in your data center or anywhere it is placed and forwards it to a convenient centralized tool farm where multiply tools can share simultaneous access to the network data" (PA0013243); and "[i]nbound traffic from any incoming port may be switched to one or more outgoing ports … Ports designated through software are Tool Ports are used to connect tools such as data recorders and VoIP monitors … the Control Panel client, a Java based graphical user interface (GUI), is proved so that the configuration and visualization of part mappings is easy and intuitive" (PA0013244). This tool optimization is depicted in Figure 1-2 on PA0013244, which is reproduced herein.

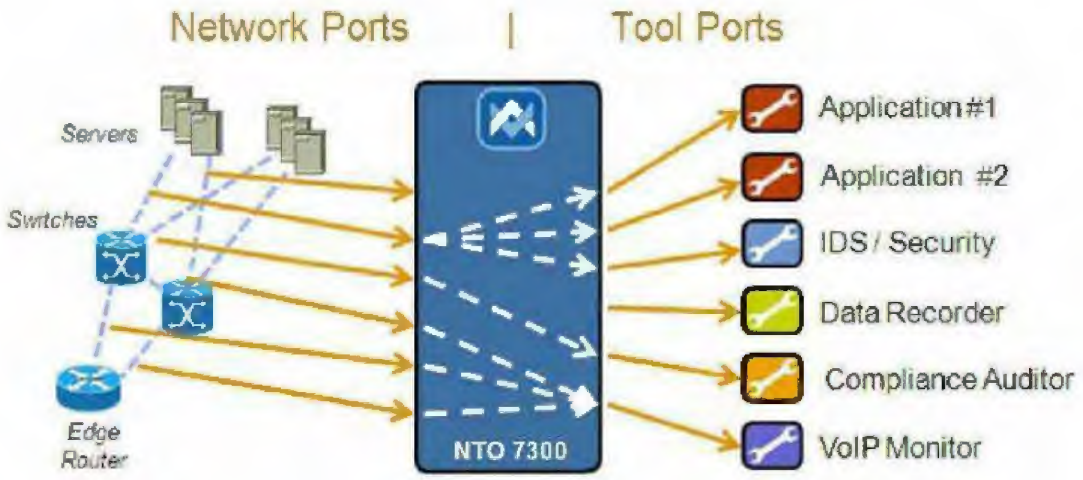


Figure 1-2. Tool Optimization through a NTO 7300 System

Figure 99 Reproduced from NTO 7300 manual (PA0013244).

537. The NTO 7300 enables various filter types to be applied, as described in PA0013247-49, which apply user-configurable rules to packets which match associated filter criteria. Packets which match applicable rules are subjected to a range of potential actions, including being allowed or denied to continue towards their destination, and/or logging.

538. The NTO filtering is configurable via a GUI, a screenshot from the Control Panel of which is provided below (reproduced from PA0013277).

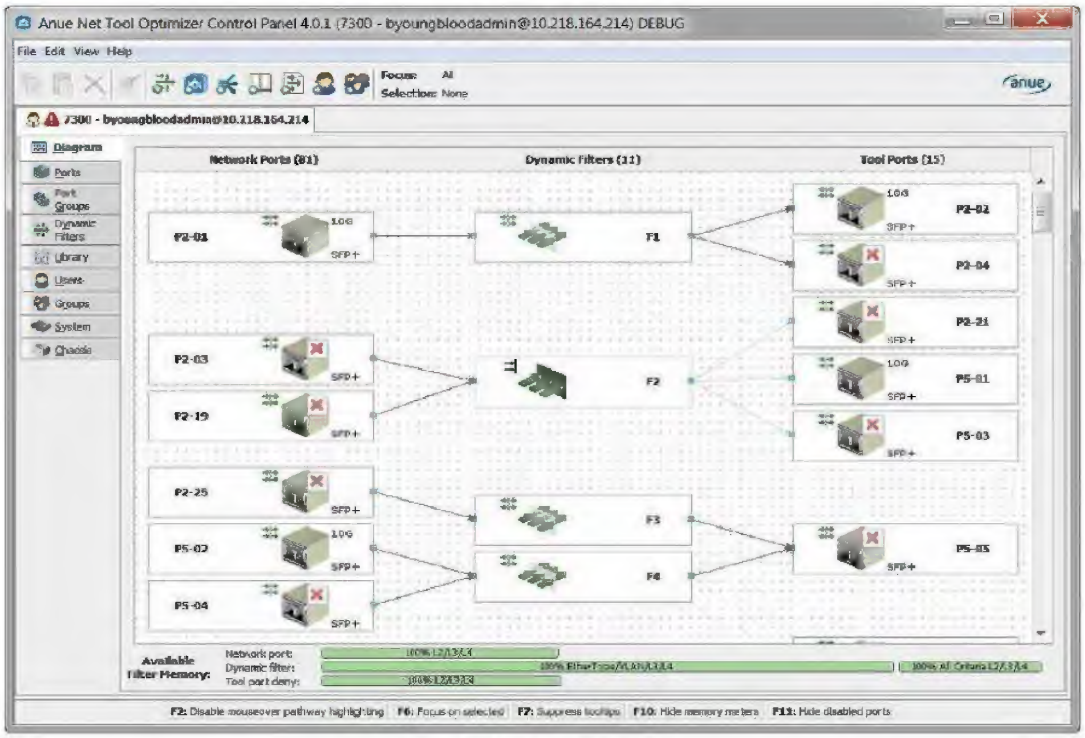


Figure 4-11. Control Panel

Figure 100. Screenshot showing the Control Panel overview of the NTO 7300 GUI (reproduced from PA0013277).

4. MOTIVATION TO COMBINE

539. The network filtering appliance of the '128 Patent, PoliWall product, and NTO 7300, are all directed towards the same field of endeavor: enhancing network security and traffic optimization. Each of these prior art systems addresses this field in a similar manner, by applying filtering to traffic on a packet-by-packet bases to enforce a policy comprised of various rules, where each rule is applicable only to packets that match certain criteria or conditions.

540. More specifically, the network filtering appliance of the '128 Patent and PoliWall both include functionality that enables filtering of packets based on their geographical origin. The '128 Patent includes example embodiments where traffic is restricted from particular

countries using a centralized server that updates lists of IP addresses associated with a given region; and also examples of using other data that is non-geographical for filtering purposes. PoliWall includes an intuitive GUI that enables a user to conveniently select IP addresses from countries and apply various rules including drop, trust (forward), or log. A POSITA would recognize that a combination of the GUI elements of PoliWall with the centralized server update mechanism, and additional non-geographical filtering criteria, of the '128 Patent would result in an improved system that overcomes shortcomings of each individual prior art. For example, the automatic updating of IP addresses using information from the Internet Name and Number regulatory authorities (*see* e.g. the '128 Patent, 3:54-63) would enable PoliWall to rapidly adapt to newly issued IP addresses, and would improve the accuracy of rules based upon country selections made via the PoliWall GUI.

541. The NTO 7300 is directed towards optimization of traffic over a large network that includes a range of different tools/functionalities. Thus, the NTO 7300 acts as a packet broker that can filter packets to reduce the load on the tools and balance the packet load among groups of tools. For example, a network may include multiple instances of a service to increase capacity and the NTO 7300 can identify packets addressed to said service and distribute them between the multiple instances to optimize the loading and thereby increase performance of said service. Alternately, a network may have several different services that each handle a different kind of traffic, and the NTO 7300 can direct appropriate packets to their corresponding service. This enables specialized tools to process relevant packets and thus increase the overall performance of a network. A POSITA would recognize that the packet brokering of the NTO 7300 can be combined with the security filtering of the PoliWall, the filtering appliance of the '128 Patent, or a combination of the two.

Furthermore, a POSITA would understand that such a combination would enable the security filtering provided by security gateways to first protect a network from threats, before the allowed traffic is subsequently optimized throughout the protected network by the NTO 7300.

542. Thus, a POSITA would recognize that a combination of the centralized server update mechanism, and non-geographical filter criteria, of the '128 Patent with the packet filtering and rule-creation GUI of the PoliWall, and network traffic optimization of the NTO 7300 packet broker functionality, would result in a system that confers benefits over and above those offered by each prior art in insolation. At least due to the mutual use of IP packets, which by their nature are designed to be compatible across numerous devices, and because this combination can be made without significant modifications to any prior art, a POSITA would understand that such a combination would be likely to succeed without undue experimentation.

543. Therefore, for at least the reasons above, it is my opinion that a POSITA would have been motivated to combine the packet filtering of the PoliWall, enhanced with the centralized server update functionality of the '128 Patent, with the network traffic optimization of the NTO 7300 packet brokering functionality.

544. As detailed below, it is my opinion that the prior art combination identified above renders obvious Claims 1 and 25 of the '722 Patent.

5. CLAIM 1

545. **Claim 1a: A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators.** The

CENTRIPETAL-CSCO 087709

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 209

prior art combination identified above includes a packet-filtering device at least because all three of the prior arts within said combination disclose devices for filtering packets. As described above in relation to each prior art, and in relation to the identified combination thereof, the packet filtering devices apply sets of rules which cause the packet filtering devices to identify packets that correspond to at least one network-threat indicator. For example, the '128 Patent discloses that IP traffic can be restricted to IP addresses which are known to be associated with certain content (e.g. pornography), and the '128 Patent and PoliWall disclose applying rules based on the origin IP address of packets to enable regions of known network-threat to be blocked while allowing traffic from trusted regions to be accepted.

546. Indeed, this claim element merely requires that a packet filtering device perform its usual and expected functionality: filter packets by applying rules to packets that match certain criteria or conditions. A POSITA would recognize that a typical usage case for a packet filtering device, which were widespread and routinely used before the priory date of the '722 Patent, is to apply said rules according to criteria related to network-threats, at least because that was a frequently adopted approach to network security.

547. Therefore, for at least the reasons above, the prior art combination identified above satisfies all requirements of this claim element.

548. **Claim 1b: receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet.** The prior art combination described above satisfies the requirements of this claim limitation, for at least the reasons below.

549. The packet filtering devices disclosed by the '128 Patent, PoliWall, and NTO 7300, are all intended to receive a plurality of packets which, in any practical usage case, will far exceed two packets. The packet-filtering device of the prior art combination identified above would typically be located such that all traffic between the network it is protecting and other networks (e.g. the Internet) is received by the packet-filtering device: thus, said packet-filtering device must necessarily receive at least two packets in normal usage.

550. Therefore, for at least the reasons above, the prior art combination identified above satisfies all requirements of this claim element.

551. **Claim 1c: responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators: applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet.** I understand that there is a dispute regarding the construction for "responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators." More specifically, Plaintiffs have proposed that this term be construed as "if the packet-filtering device determines the first packet meets one or more conditions associated with one or more network threat indicators from a packet filtering rule," while Defendants propose that no construction is needed and this term should be given its "plain meaning." I have considered both proposed construction in my analysis, and reserve the right

to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination identified above satisfies all requirements of claim element 1c, for at least the reasons below.

552. I also understand that there is a dispute regarding the construction of the term "operator." More specifically, Plaintiff has proposed that this term be construed as "an adjustable instruction that causes the packet filtering device to either prevent or allow a packet to continue to a destination," while Defendants have proposed that this term be construed as "function to either prevent a packet corresponding to criteria from continuing or allow it to continue to its destination." I have considered both proposed claim constructions in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination described above satisfies all requirements of claim element 1c, for at least the reasons below.

553. This claim element requires that the packet-filtering device identify the first packet as matching a rule which results in the packet-filtering device forwarding the packet toward its destination. The '128 Patent discloses "trusted lists" for which traffic is allows, which constitutes rules that allow matching packets to continue to their destination. In addition, the PoliWall product enables creation of geographical regions from which packets are allowed to continue to their destination; for example, the PoliWall YouTube video[66] includes an example of creating a rule that enables traffic from North America to be accepted and forwarded to its destination, and a different example of creating an exception within a blocked region such that packets from the IP addresses included in the exception will be forward to their destination even though other traffic from the same country will be blocked.

554. Furthermore, a POSITA would recognize that the requirements of claim element 1c are commonly applied by packet-filtering devices during their typical usage cases. For example, specifying a set of known IP addresses from which packets may be trusted and forwarded to their intended destination is a common way of reducing load on security filters: packets from known and trusted locations (e.g. other offices of the same business) may be forwarded safety with less scrutiny than packets from other IP addresses, thus reducing the load on the filtering system because after packets are identified as being trusted they may not need to be compared against other filtering rules. Thus, a POSITA would understand that the prior art combination identified above would typically be used in a way that satisfies all requirements of claim element 1c.

555. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 1c.

556. **Claim 1d. communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;** I understand that there is a dispute regarding the construction for the term "communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet." More specifically, Plaintiff has proposed that this term be construed as "causing a packet-filtering device to generate and communicate a record that identifies (1) a network threat indicator based on a rule and (2) data that indicates that the first packet was allows to continue toward the destination," while defendants have proposed that no construction is required and this term

should be given its "plain meaning." I have considered both proposed claim constructions in my analysis, and reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination identified above satisfies all requirements of this claim, as detailed below.

557. Regardless of which construction is applied, the requirements of this claim element are satisfied by a packet-filtering device that may log a network threat indicator that is associated with a packet because said packet matches the criteria, or conditions, or a rule, while forwarding said packet to its intended destination.

558. The '128 Patent discloses logging of packets that are forwarded to their destination. For example, the '128 Patent states, in relation to a chain of rules that may be applied to matching packets, "[i]f the packet is not matched by any of the above chains, the packet details are logged 290 and the packet is accepted 500" (the '128 Patent, 7:8-9). The '128 Patent also discloses a GUI that displays real-time statistics which may relate to which IP addresses accessed a system. The information displayed on the GUI can be customized by the user to their preferences (*see* the '128 Patent, 8:36-48). In addition, the '128 Patent discloses "Clickable Real-Time Logs" which can hold information for each packet that is filtered, or "attached additional information based on the packet details"; and, the Real-Time Logs may be made available via a "real-time display" that "is updated every second and shows information about the packets traversing the system" (*see* the '128 Patent, 8:50-26).

559. The NTO 7300 provides extensive logging of packets which are forwarded to their intended destination service. A key functionality of the NTO 7300 is to monitor and log information about traffic to enable, for example, optimization of its rules.

560. Furthermore, a POSITA would recognize that logging of packets that match the criteria of a rule is a widespread and commonly applied feature of typical packet-filtering devices. Thus, a POSITA would understand that any packet that matches the criteria of a rule, where said rule is configured to forward the packet to its destination, would satisfy the requirements of claim element 1d; and, that such rules have many applications, e.g. for flagging trusted IP addresses.

561. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 1d.

562. **Claim 1e: causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;** I understand that there is a dispute regarding the construction for "interface." More specifically, Plaintiff has proposed that this term be construed as "plain and ordinary meaning," while Defendants have proposed that this term be construed as "a display visible to the user that allows a user to provide input." I have considered both proposed constructions in my analysis, and I reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination identified above satisfies all requirements of claim element 1e, as detailed below.

563. The GUI of PoliWall, which is a "display visible to the user" enables the user to click on an interactive map to apply rules to traffic from selected countries. Thus, this constitutes "allow[ing] the user to provide input." Thus, GUI of PoliWall satisfies the construction proposed by Defendants. In addition, the GUI of PoliWall would be understood by a

POSITA to satisfy the plain and ordinary meaning of an interface, at least because it provides a typical web-browser based display that enables a user to click to select elements.

564. The NTO 7300 also includes an extensive user interface that satisfies both constructions. For example, the interface is used to enable configuration of the filtering rules, which satisfies Defendants' proposed construction; and, a POSITA would recognize the interface as a typical GUI, satisfying Plaintiff's proposed construction.

565. A POSITA would understand that a typical approach to displaying log information involves tabulated data that often includes the network-threat indicator, or the corresponding rule, that caused a packet to be filtered and logged, along with other information related to said packet.

566. Therefore, for at least the reasons above, it is my opinion that the prior art combination described above satisfies all requirements of claim element 1e.

567. **Claim 1f: receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and.** I understand there is a dispute regarding the construction of the term "user." More specifically, Plaintiff has proposed that this term be given its "plain and ordinary meaning," while defendants have proposed that this term be construed as "person (e.g., administrator)." I have considered both claim constructions in my analysis, and reserve the right to modify my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of this claim. In any event, it is my opinion that the plain and ordinary meaning of the term "user" includes "person (e.g., administrator).

568. The PoliWall YouYube video[66] includes example of a person (who is a "user") invoking elements of the PoliWall GUI which results in rules being created or updated. Thus, a POSITA would recognize that the GUI us being used to generate instructions for the packet-filtering device in response to user input via invoking elements of said GUI (e.g. clicking on countries in the video). Indeed, the video demonstrate an immediate change in behavior of the packet-filtering device in response to instructions generated by invocation of the GUI, and thus the packet-filtering device must necessarily be receiving said instructions.

569. The user manual for the NTO 7200 includes numerous screen shots showing how a user can manipulate, or otherwise invoke, elements of the GUI to configure network rules. A POSITA would recognize that the GUI is generating instructions which correspond to the user's action and that these must necessarily be received by the packet-filtering device in order for it to function as intended.

570. Furthermore, a POSITA would understand that the use of GUI elements to interact with a hardware device was widespread, and is a typical means by which packet-filtering device are configured. Also, at least because a significant aspect of configuring packet-filtering devices involves creation or modification of packet-filtering rules, or network-threat indicators used by rules, a POSITA would expect that a typical GUI for a packet-filtering device would include mechanisms for doing so.

571. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 1f.

572. **Claim 1g: responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria**

from continuing toward their respective destinations; and. I understand that there is a dispute regarding the construction of the term "modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their destination." More specifically, Plaintiff has proposed that this term be construed as "modifying the state of the packet-filtering device to cause an adjustable instruction to prevent a packet from continuing toward its destination," while Defendants propose that no construction is required and this term should be given its "plain meaning." I have considered both proposed constructions in my analysis, and I reserve the right to amend my analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the prior art combination identified above satisfies all requirements of claim element 1g, as detailed below.

573. A POSITA would understand that modification of a packet-filtering rule is commonplace and frequently performed in order to improve the performance of said packet-filtering device, or in response to changes in network traffic. For example, if a new trusted IP addresses becomes known (e.g. if a company opens an office in a new location) rules would typically be created or modified in order to correctly handle packets from this new office; similarly, if an IP address is becomes compromised (e.g. unwanted traffic is frequently detected from said IP address) a rule may be modified to block packets from this address. A POSITA would further understand that such modifications are routinely made via the GUI associated with a packet-filtering device; and thus, that instructions may be received by the packet-filtering device that are generated in response to a user invoking elements of the GUI.

574. Indeed, the PoliWall video[66] includes a demonstration of modifying a rule in order to prevent traffic from certain IP addresses from being forwarded: in the video, traffic that was previously being forwarded is shown to no longer be forwarded after the GUI has been invoked to modify a rule. Thus, the PoliWall video demonstrates the requirements of claim element 1g are satisfied by the prior art combination identified above.

575. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 1g.

576. **Claim 1h: responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria: preventing by the packet-filtering device, the second packet from continuing toward a destination of the second packet;** The prior art combination identified above satisfies all requirements of this claim element for at least the reasons below.

577. A POSITA would understand that preventing a packet from reaching its destination if a common result of packet filtering if, for example, a packet-filtering device determines that said packet corresponds to criteria of a rule that results in packets being dropped.

578. Indeed, dropping of packets that match the criteria of rules is a key feature of the packet filtering appliance of the '128 Patent, and also of PoliWall (e.g. *see* the YouTube video[66] for demonstrations of packets being prevented from reaching their destination if they match the criteria of rules).

579. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 1h.

580. **Claim 1i: communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second**

packet; and. For at least the same reasons as detailed in relation to claim element 1d, e.g. those relating to logging functionality, it is my opinion that the prior art combination identified above satisfies all requirements of this claim element.

581. In addition, a POSITA would recognize that the requirements of this claim are typical features of packet-filtering devices, at least because it is common practice for packet-filtering devices to log packets that are dropped, or otherwise match rules, and that logs are typically made available to users.

582. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all elements of claim element 1i.

583. **Claim 1j: causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.** For at least the reasons detailed in relation to element 1e, the prior art combination identified above satisfies element 1j.

584. Furthermore, a POSITA would recognize that logging of filtered packets is a standard practice that is typically performed by packet-filtering device; and, that the resulting logs are typically displayed via a GUI.

585. Therefore, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies all requirements of claim element 1j.

586. Consequently, for at least the reasons above, it is my opinion that the prior art combination identified above satisfies each and every element of claim 1 of the '722 Patent; and thus, it is also my opinion that Claim 1 of the '722 Patent is rendered obvious in view of this combination.

6. CLAIM 25

587. **Claim 25: The method of Claim 1, wherein: receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices.** This claim is dependent upon Claim 1 of the '722 Patent, and as detailed above it is my opinion that Claim 1 is obvious in view of the prior art combination identified above. As detailed below, the prior art combination identified above also satisfies all limitations added to Claim 1 of the '722 Patent by Claim 25 therein.

588. As detailed in relation to Claim 1, the prior art combination identified above constitutes a "packet-filtering device" as required by Claim 25 and the relevant claim constructions; and, also as detailed in relation to Claim 1, uses "packet-filtering rules" as required by Claim 25 and the relevant claim constructions.

589. The '128 Patent discloses a packet filtering appliance receiving rules from a centralized server, which constitutes "one or more computing" devices. Furthermore, the '128 Patent states "[t]he at least one appliance, server, and computer may be in operable communication with each other or with other appliances, servers and/or computers in any manner such as through a network as appreciated by one skilled in the art." Thus, the use of a centralized server, or servers, to provide packet-filtering rules to one or more packet-filtering devices would be obvious to a POSITA. For example, the use of a "centralized" server implies that said server may be used to communicate rules, and/or other information, to a plurality of distributed packet-filter devices. Indeed, such an arrangement would be well within the capabilities of a POSITA, and a POSITA would be motivated to implement such a

CENTRIPETAL-CSCO 087721

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 221

configuration at least to enable multiple packet-filtering devices to protect various network boundaries based on centralized network-threat information.

590. Therefore, for at least the reasons above, it is my opinion that Claim 25 of the '722 Patent is rendered obvious by the prior art combination identified above.

XIII. U.S. PATENT NO. 9,565,213

591. I have been asked to review the '213 Patent and assess the validity of Claims 1 and 3. I will first summarize the '213 patent briefly and then discuss claim-by-claim invalidity analysis.

A. SUMMARY OF THE '213 PATENT

592. The '213 patent assigned to Centripetal Networks, Inc., Herndon, VA (US), was filed on Apr. 16, 2014 and published on Feb. 7, 2017. The '213 patent relates to methods and systems for protection of secured network. Specifically, it relates to packet filtering of network traffic using security policy management (SPM) servers and packet security gateways (PSGs). Figure 101 illustrates an exemplary network environment protected using the methods and systems disclosed in '213 patent. In this example, there are four PSGs located at the borders of four LANs (local area networks). These PSGs protect respective networks from the incoming packets sent by a WAN (wide area network, e.g. internet). This example also includes one SPM server that communicates dynamic security policies to PSGs.[106]

[106] '213 Patent at 4:27 – 5:40.

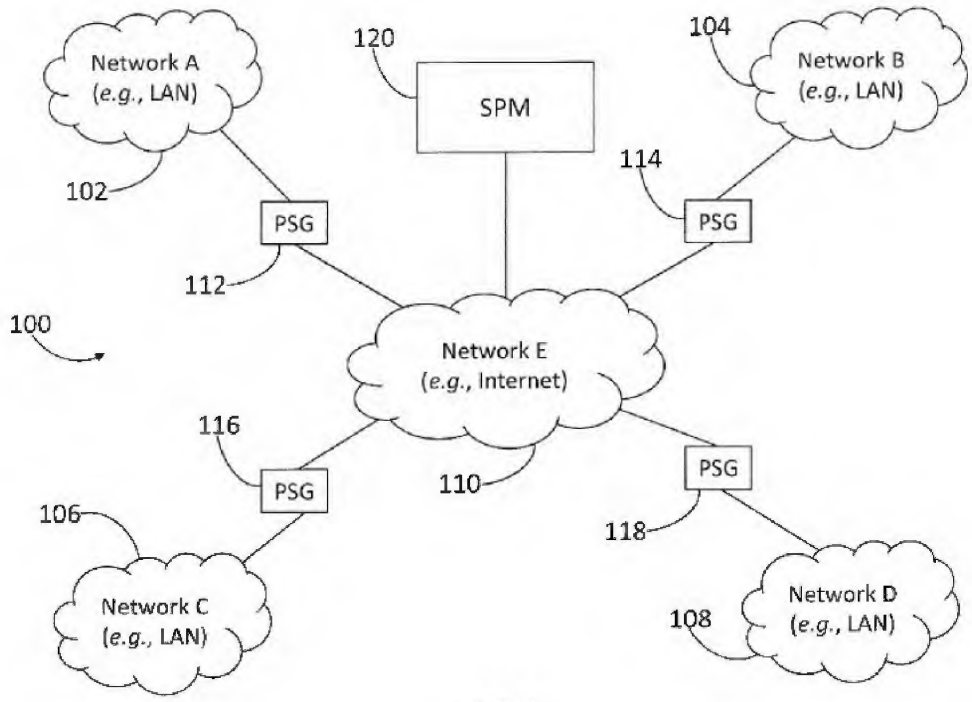


FIG. 1

Figure 101. An exemplary network environment protected by methods and systems disclosed in the '213 patent, ('213 Patent, FIG. 1).

593. A security policy management server is a computing device that is configured to communicate a dynamic security policy to a packet security gateway.[107] Figure 102 illustrates an exemplary SPM including memory, processor, management interface, and network interface (NI). The memory in SPM stores various program modules and dynamic security policies, which include criteria corresponding to one or more packets and a packet transformation function to be performed on packets corresponding to the specified criteria.[108] The processor executes program modules to configure SPM to (1) communicate dynamic security policies to PSGs, (2) receive updates from malicious host tracker service, and (3) automatically alter or create one or more rules related to malicious network traffic. The

[107] '213 Patent, at 4:53-55.
[108] '213 patent, at 4: 58-63.

management interface provides administrators access to SPM via a graphical user interface (GUI) or a command line interface (CLI). Administrators can use management interface to add PSGs and to construct new dynamic security policies. The NI interfaces SPM with the network environment and facilitates communication between SPM and PSGs.[109]

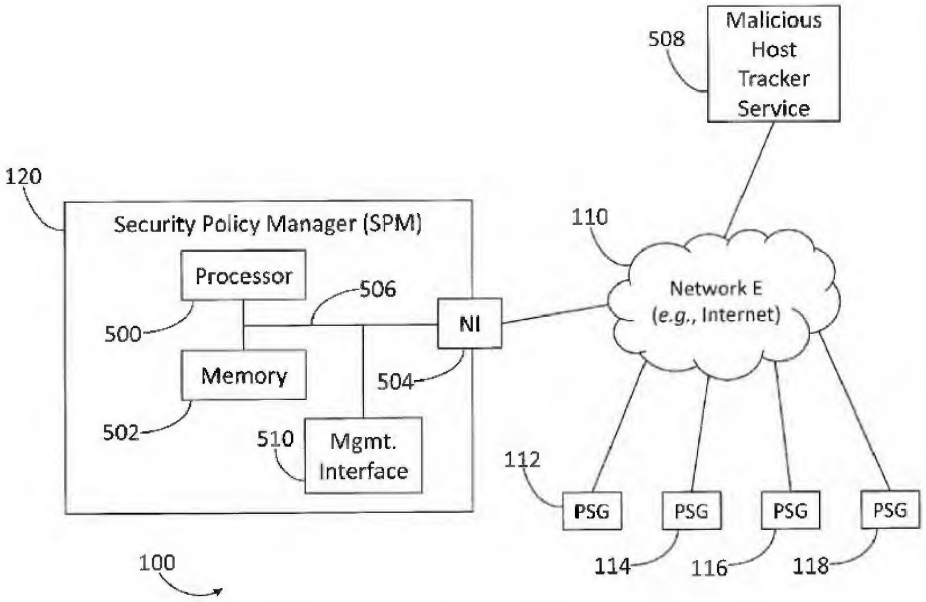


FIG. 5

Figure 102. An exemplary security policy manager (SPM) disclosed in the '213 patent ('213 Patent, FIG. 5).

594. A packet security gateway is a computing device configured to receive packets and perform a packet transformation on the packets.[110] Figure 103 illustrates an exemplary SPG including the following components: processor, memory, NIs, management interface and packet filter. The processor configures SPG by executing one or more program modules included in the memory. PSG receives dynamic security policies from SPM via the management interface or the network interface. Packet filters examine dynamic security

[109] '213 patent, at 13:57 - 15:5
[110] '213 Patent, at 4:48-50.

policy and information associated with the packets received by PSG. Based on the results of this analysis, packet filters send the packets to one or more packet transformation functions (PTF), e.g., forward or drop.[111] A PTF may also produce a digest version, or log, of the packet. Such logs can contain selected information about the packet and the system, e.g. associated network addresses, ports, protocol types, and URIs. The logs are stored or forwarded using a logging system based on a standard (e.g., syslog or the like), such that they can be used for generating awareness information.[112]

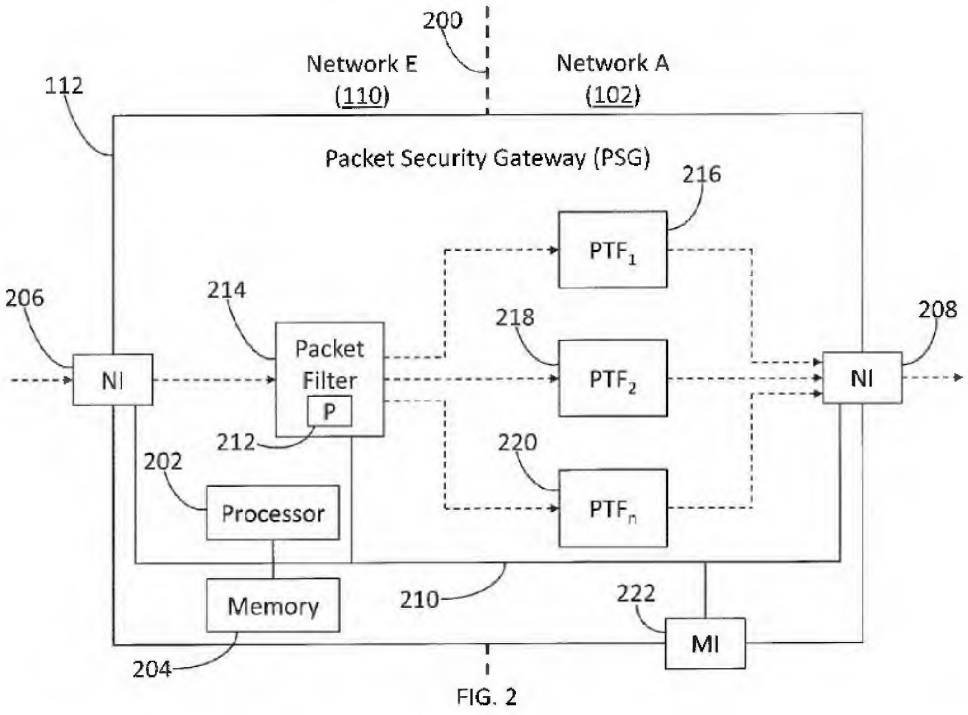


FIG. 2

Figure 103. An exemplary packet security gateway (PSG disclosed in the '213 patent ('213 Patent, FIG. 2).

595. Dynamic security policies received by PSGs include rules that specify packet-identification criteria and PTF to be performed on the packets that correspond to these

[111] '213 patent, at 5:41-6:31
[112] '213 patent, at 11:58-60

criteria. These packet identification criteria can be based on application-layer packet-header information. For example, header information for application-layer hypertext transfer protocol (HTTP) packets may include methods (e.g. PUT or GET) and URIs for transferring resources (e.g. files).[113]

B. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF TIPPINGPOINT IPS

596. The TippingPoint UnityOne-200 Intrusion Prevention System ("TippingPoint IPS" or "TippingPoint system") is a network security solution to protect virtual and physical networks, applications, and data against a range of network security threats. This system performs the functions of two packet security gateways and one security policy management server. This system performs the functions of two packet security gateways and one security policy management server, and a typical usage case for the system is to identify packets that correspond to criteria so that a criteria-specific action (e.g. blocking, logging, forwarding, re-routing, or the like) may be applied on a packet-by-packet basis to network traffic.

597. The TippingPoint system was commercially available to purchase before the priority date of the '213 Patent, and I have been informed by counsel that the TippingPoint system constitutes prior art.

598. For at least the reasons detailed below, it is my opinion that the TippingPoint system enabled a person of ordinary skill in the art to practice each and every element of Claims 1 and 3 of the '213 Patent, and that a POSITA would be motivated to do so as part of the typical routine of setting up standard network protection mechanisms. Thus, it is also my opinion that the TippingPoint IPS anticipates these claims. In addition to the analysis presented herein, further discussion of relevant testing is described in Appendix F, which I incorporate by reference.

[113] '213 patent, at 7:49-67

1. TEST CONFIGURATION WITH TIPPINGPOINT IPS

599. Exponent procured a TippingPoint IPS device with part number SBASY-199 Rev: C03 and serial number ST05170004, as shown in Figure 104.



Figure 104. TippingPoint IPS hardware showing the part number and serial number of the device.

600. The TippingPoint system includes a local security manager (LSM) program, which "is the control center from which you can configure, monitor, and report on the UnityOne Intrusion Prevention System (IPS) devices in your network."[114] The TippingPoint IPS also includes two separate Ethernet port pairs called "segments"; each segment can be programmed to follow its own set of filtering rules via the LSM.

601. The TippingPoint IPS LSM includes "a graphical user interface (GUI) that enables you to monitor and configure your UnityOne Intrusion Prevention System (IPS) using an ordinary

[114] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. xi.

web browser."[115] For Exponent's testing, a computer running Windows XP was connected via Ethernet cable to the MGMT Ethernet port of the TippingPoint IPS, which is indicated with red annotations in Figure 105, and Internet Explorer 7 was used to access the TippingPoint IPS GUI from this computer.[116]



Figure 105. Annotated photographs of the TippingPoint IPS showing two packet security gateway interfaces (lower left) and one management interface (lower right).

602. The physical configuration of the test setup used for Exponent's analysis is shown in Figure 106. This figure shows the physical layout of the hardware, including the IPS with its two segments (SEG 1 and SEG 2), the computer used to connect to the LSM interface (labeled "LSM"), two switches, and three additional laptop computers (Computers A, B, and C) for sending and receiving packet traffic.

115 "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 8.

116 The TippingPoint IPS web server was found to be incompatible with modern versions of Internet Explorer. Internet Explorer 7 was released circa 2006. (See, for example, https://en.wikipedia.org/wiki/Internet_Explorer_version_history#Windows_Internet_Explorer_7.)

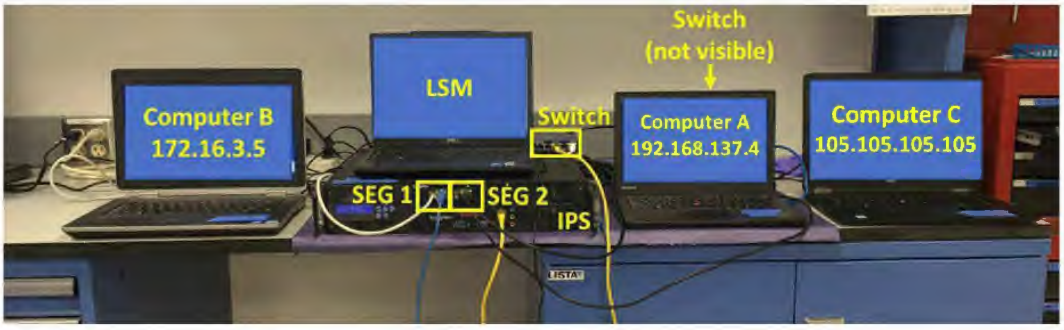


Figure 106. Image of test network used as part of the claim analysis that shows a hardware installation of one IPS containing a local security management (LSM) interface. The laptop labeled LSM is used to connect to the LSM. Computers A, B, and C reside in separate network address spaces and are connected by the two segments.

603. The test configuration shown above includes computers with IP addresses in three different network address spaces.

604. A first network, called "Network A," includes IP addresses in the range from 192.168.1.37.2 through 192.168.137.5, which contains Computer A. Network traffic internal to Network A is communicated via a TP-Link TL-SG108 Switch (not visible in Figure 106). A second network, called "Network B," includes a computer with IP address 172.16.3.5, which is Computer B. Network A and Network B are connected by the first segment, which is the segment labeled SEG 1 in Figure 106.

605. The test network shown in in Figure 106 also includes a third network, called "Network C," that includes a computer with IP address 105.105.105.105, labelled "Computer C." Network A and Network C are connected by the second segment, which is the segment labeled SEG 2 in Figure 3.

606. Figure 107 shows the schematic layout of the networks described above. Network A includes Computer A, as well as other IP addresses as indicated in the figure; Network B includes Computer B; and Network C includes Computer C. The first Tipping Point system

segment (SEG 1) protects Network B from Network A; and the second segment (SEG 2) protects Network C from Network A.

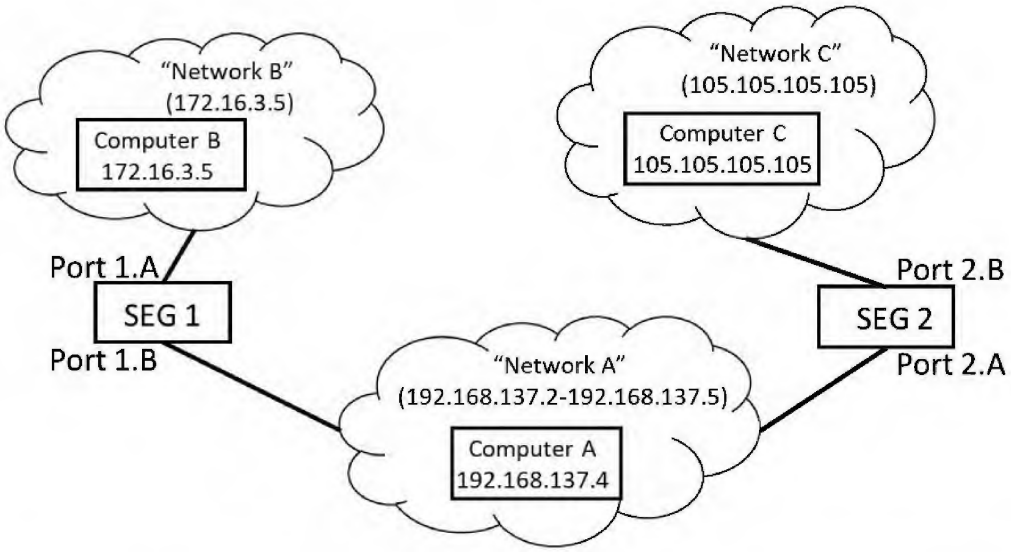


Figure 107. Schematic of the test network (see Figure 106) architecture, including the static IP addresses of each element. Each network has its own subnet. SEG 1 protects Network B from Network A. SEG 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (Port A and Port B), which are used to pass traffic between networks

2. CLAIM 1

607. **Claim 1a: A method comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

608. I understand there is a dispute regarding the construction of the term "dynamic security policy," in relation to the '213 Patent. More specifically, in the Joint Claim Construction

CENTRIPETAL-CSCO 087730

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 230

Statement[117] Plaintiff has proposed that this term be construed as "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets," while Defendants have proposed that this term be construed as "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria".[118] According to the '213 Patent specification, "[a] dynamic security policy includes any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria."[119] I have considered both proposed constructions in my analysis in addition to the description of this term within the '213 Patent specification, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of this claim element, for at least the reasons detailed below.

609. The '213 Patent states that "[a]s used herein, a security policy management server includes any computing device configured to communicate a dynamic security policy to a packet security gateway."[120] I understand that the parties have agreed that the term "security policy management server" is to be construed as "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway."[121] For my analysis I have considered the agreed upon construction of the term "security policy management server" as well as the description of this term within the '213 Patent specification and I

[117] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))
[118] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.
[119] '213 Patent, Column 4, Lines 58–63.
[120] '213 Patent, at 4:53-55.
[121] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.

reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system comprises a security policy management server, for at least the reasons detailed below.

610. The TippingPoint system includes a local security manager (LSM) program, which "is the control center from which you can configure, monitor, and report on the UnityOne Intrusion Prevention System (IPS) devices in your network."[122] As detailed in relation to Figure 105, the LMS program is accessed via a web server running on the MGMT Ethernet interface of the TippingPoint IPS. As detailed below, this server enables access to a graphical user interface (GUI) with which dynamic security policies may be managed and communicated to the TippingPoint security gateways. Therefore, the TippingPoint includes "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway," as required by the claim construction of "security policy management server." The TippingPoint system also satisfies the definition for "security policy management server" stated within the '213 Patent, at least because the laptop running the TippingPoint LSM constitutes a "computing device configured to communicate a dynamic security policy to a packet security gateway," which is broader than the agreed upon construction.

611. The '213 Patent states that "[a]s used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation on the packets."[123] I also understand that the parties have agreed that the term "packet security gateway" is to be construed as "a gateway computer configured to receive packets and

[122] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. xi.
[123] '205 Patent, at 4:48-50.

perform a packet transformation function on the packets."[124] I have considered both the agreed upon construction as well as the description within the patent specification throughout my analysis, and regardless of which construction is applied, it is my opinion that the TippingPoint system includes "a plurality of packet security gateways," for at least the reasons below.

612. The TippingPoint system includes two separate Ethernet port pairs called "segments," which are labeled "SEG 1" and "SEG 2" in Figure 105, that act as two separate packet security gateways where each security gateway can be programmed independently to follow its own set of filtering rules via the LSM. For example, as discussed in relation to Figure 105 and Figure 106, each security gateway segment receives packets traveling between networks, and then applies filtering rules to these packets. More specifically, in Exponent's test setup described above, segment 1 is located at the boundary between Network A and Network B, and receives all packets that pass between these two networks. Upon receiving packets, a computer within the TippingPoint IPS applies rules according to the currently applied security policy. Thus, the TippingPoint system includes "a gateway computer configured to receive packets" as required by the agreed upon construction for "packet security gateway." The TippingPoint system also satisfies the requirement of including "a plurality of packet security gateways" in accord with the description of a "packet security gateway" stated within the '213 Patent, at least because the laptop running the TippingPoint LSM constitutes a "computing device configured to receive packets and perform a packet transformation on the packets," which satisfies the agreed-upon construction for this term.

613. Furthermore, the TippingPoint security gateway segments are each "associated with the security policy management server" at least because the security policies, and associated

[124] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.

rules, applied by each segment are configurable using the LSM program via the webserver running on the MGMT Ethernet interface.

614. I also understand that there was a dispute regarding the construction of the term "packet transformation function." More specifically, in relation to the '213 Patent, Plaintiffs proposed that this term be construed as "function that transforms packets from one state to another" while Defendants proposed "an operation performed on a packet specified by the dynamic security policy, such as forward or drop."[125] I have considered both proposed constructions in my analysis, as well as the example embodiment of packet transformations described within the '213 Patent specification, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies the requirements for this term for at least the reasons discussed herein.

615. Plaintiff's proposed construction of "packet transformation function" requires a function that "transforms one or more packets from one state to another." Although Plaintiff's did not provide an explicit definition for transforming "from one state to another," the intrinsic evidence cited to by Plaintiff in support of their proposed construction included example embodiments in which packets are forwarded or dropped depending upon parameters of the packet such as the origination IP address. Thus, under Plaintiff's proposed construction, forwarding or dropping of packets constitutes transforming a packet from one state to another, and hence forwarding or dropping satisfy Plaintiff's construction of "packet transformation function." Similarly, Defendants' proposed construction for "packet transformation function" explicitly includes the operations "forward or drop," and hence forwarding or dropping also satisfy Defendant's proposed construction for this term.

[125] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

616. Amongst example embodiments provided by the '213 Patent specification, "packet transformation functions," specified by the dynamic security policy, include forwarding, dropping, logging, or routing packets to a network address different from a packet's destination network address (i.e. rerouting) (*see* '213 Patent, col 2:36-59 and col 11:45-48).

617. As detailed below, the TippingPoint IPS can perform a variety of functions upon the received packets, depending upon the rules within the current policy and parameters of the received packets, including but not limited to: forwarding packets to their intended address; forwarding packets to an address other than their intended address; dropping packets; logging or otherwise monitoring packets. Therefore, the TippingPoint IPS satisfies all constructions for "packet transformation function."

618. Although the TippingPoint IPS is capable of performing a variety of different "packet transformation functions," in accord with the proposed constructions of said term, the limitations of claim element 1a specifically requires that the packet transformation function "compris[e] a packet digest logging function to be performed on packets comprising the application-layer packet-header information." The TippingPoint software application which enables the implementation of packet filtering rules constitutes an "application layer." I understand, however, that the parties have agreed that the term "packet digest logging function" is to be construed as "a function that identifies a subset of information for a packet and generates a record," and that the term "application-layer packet-header information" is to be construed as "information in the header of a packet that corresponds to the application-layer." These are consistent with the plain and ordinary meaning of packet-header information, which is the portion of a packet that precedes its body and contains addressing and other data that is required for it to reach its destination; and also with the '213 Patent

specification, which includes a variety of examples of "application-layer packet-header information," stating "For example, application-layer hypertext transfer protocol (HTTP) packets … may contain headers that specify methods and/or one or more uniform resource identifiers (URIs) for transferring resources (e.g. files) between client and servers" ('213 Patent, col 7:49-55). The '213 Patent specification also states that a "packet digest logging function" is a type of packet transformation function, specified by a rule, that "when applied to a packet that matches such a rule, produces a digest version, or log, of the packet. This packet log (or digest) may contain selected packet information and/or system information" ('213 Patent, col 11:47-50). As noted above, and discussed in greater detail below, the TippingPoint IPS can perform packet transformation functions that include packet logging. Thus, the TippingPoint system can perform the requirements of this claim element in accordance with the agreed upon constructions and the '213 Patent specification, therefore satisfying the limitations of this claim element.

619. It is my understanding that no claim construction has been submitted for the term "rule," with respect to the '213 Patent, and thus the plain and ordinary meaning should be applied. However, it is also my understanding that there was a dispute regarding the construction of this term in the Joint Claim Construction Statement[126] with respect to the '205 and '077 Patents. While I have applied the plain and ordinary meaning to the term "rule" for the '213 Patent, because the '213, '205, and '077 Patents have similar specifications, with similar or identical terms in the claim language, and address similar subject matters at similar points in time as would be understood by a similar POSITA, I have also considered the respective claim constructions addressed in the Joint Claim Construction Statement while performing my analysis herein.

[126] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))

620. I understand that, with respect to the '205 and '077 Patents, Plaintiff has proposed that this term be construed as "condition or set of conditions that when satisfied cause a specific action to occur," while Defendants have proposed that this term be construed as "(i) packet-identifying criteria and (ii) a function to be performed on the identified packets."[127] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the TippingPoint system satisfies all requirements of this claim element, for at least the reasons detailed below.

621. As discussed in relation to this claim element, the TippingPoint system is able to implement rules that specify a set of criteria for which packets should be forwarded, dropped, and/or logged. These rules satisfy both the proposed claim constructions. For example, these rules contain a "condition or set of conditions" based upon, for example, packet-header information associated with received packets, as discussed above, and cause "a specific action to occur" (e.g. forward or drop) when packets satisfy said condition or set of conditions: thus, Plaintiff's proposed construction is satisfied. Also, for these rules the packet-header information of received packets may be used as "packet-identifying criteria," and "a function" (e.g. forward or drop) is "performed on the identified packets": thus, Defendants' proposed construction is also satisfied.

622. Using the test setup described above, Exponent has demonstrated that the TippingPoint security gateway segments receive dynamic security policies from the LSM and associated web server. The TippingPoint system includes 1,888 filters that are available via default on the TippingPoint IPS, 15 of which are shown in Figure 108. Each of these filters comprise at least one rule that can be adjusted to perform various user-defined packet transformation

[127] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

functions upon packets associated with said rule, e.g. forwarding, dropping, logging, copying, etc., on packets that correspond to relevant criteria[128]: i.e. each filter, which constitutes at least one rule, contains at least one criteria, and at least one packet transformation function that is to be applied to packets that are associated with filter by satisfying said criteria. Thus, each filter comprises at least one rule that satisfies both the proposed constructions for "dynamic security policy."

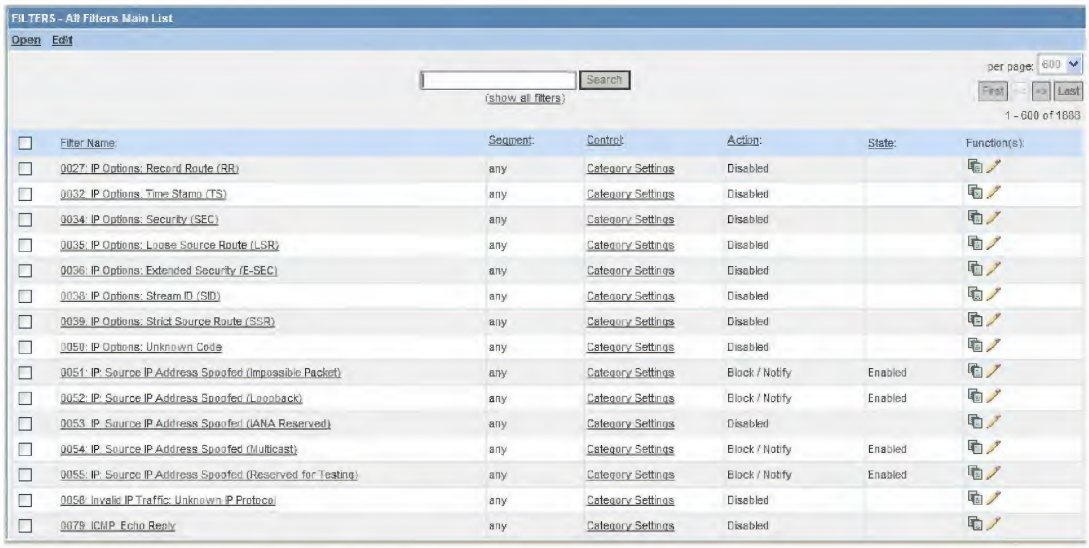


Figure 108. Sample filters available in the IPS.

623. For example, Figure 109 below shows a screen shot from the settings window, accessed via the LSM GUI, for a filter called "0361:HTTP:Protected File Access (/etc/passwd)." The HTTP Protected File Access filter applies to application-layer packet-header information. In this case the application-layer protocol is HTTP and the header information is the method (e.g., GET) and the URL path ("/etc/passwd"). This filter detects HTTP requests that are attempting to access the password file on a Unix system, which is typically stored in file

[128] See, "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 23, Section 3 "Filters."

/etc/passwd: i.e. the criteria for this filter is satisfied by any packets that are attempting to send a request to access /etc/passwd.

624. The dropdown menu that is also shown in this figure contains a list of "actions" that can be selected: these actions define the packet transformation function that will be performed upon packets that match the criteria of the filter. The "save" button in the lower right corner updates the filter settings.

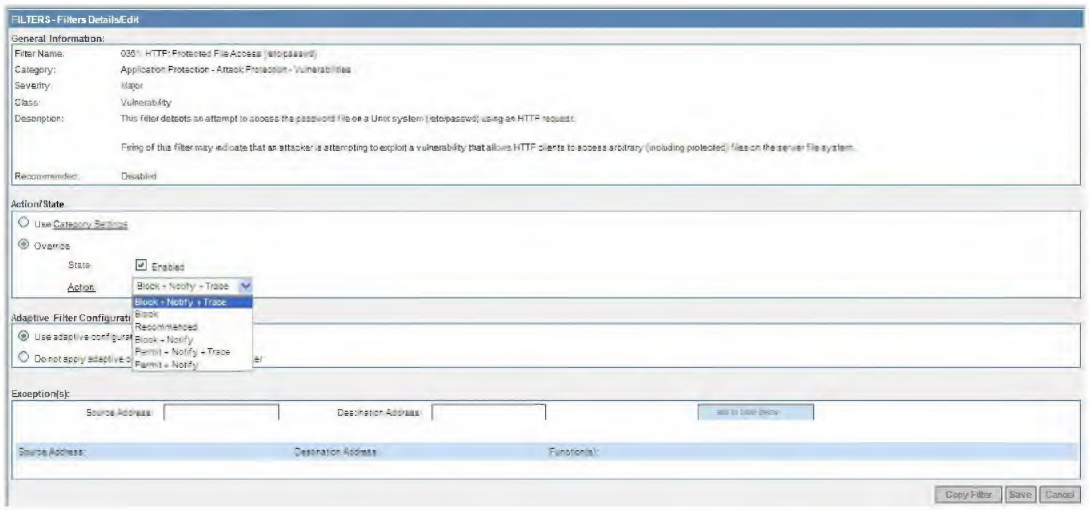


Figure 109. Filter 0361, which "detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request." A series of actions are possible for packets that are identified by this filter.

625. That the available "actions" correspond to packet transformation functions has been confirmed via Exponent's testing. For example, as seen in Figure 109, the action taken by this filter can be set to "Block + Notify + Trace," which applies a packet transformation function to each packet that matches the application-layer packet-header pattern. The packets that match the filter criteria associated with the application-layer packet-header information are prevented from reaching their intended destination (i.e. are "blocked"). Furthermore, blocked packets are intercepted and logged in a Block Log, as is shown in Figure 110, after a single packet that matches the 0361:HTTP:Protected File Access

(/etc/passwd) filter criteria while the appropriate action was set, thus demonstrating that a packet digest logging function is included in the packet transformation function performed on the HTTP application-layer packet-header information.

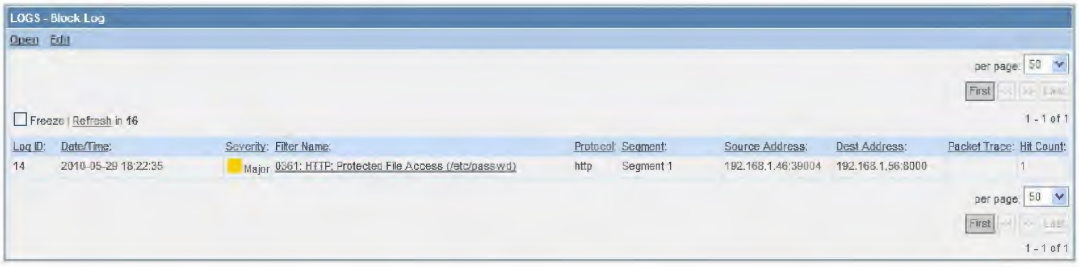


Figure 110. Block Log, which shows the blocked packets.

626. Thus, as explained above, The TippingPoint system may contain a "plurality of packet security gateways associated with a security policy management server," wherein the packet security gateways receive "a dynamic security policy" from the TippingPoint LSM and associated web server, "that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information." As demonstrated above, the 0361:HTTP:Protected File Access (/etc/passwd) filter implements such a rule that can perform a packet digest logging function on packets comprising the application-layer packet-header information.

627. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1a of the '213 Patent.

628. **Claim 1b: receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

629. The first TippingPoint system security gateway segment (SEG 1) is located at an interface between Network A, which contains Computer A, and Network B, which contains Computer B, as shown in the test configuration setup in Figure 106. This packet security gateway protects Network B from Network A, while the second segment (SEG 2) protects Network C, which contains Computer C, from Network A.

630. To demonstrate the functionality required by this claim element, ping attempts were made between Computer A and Computer B. More specifically, an attempt was made to ping Computer A from Computer B. These ping requests were allowed to transmit indicating that Segment 1 was forwarding packets from Computer B to Computer A as well as from Computer A to Computer B. Figure 111 is a screenshot of Computer B's successful attempt to ping Computer A. Note that by default a command line "ping" function makes four ping requests, as seen in the screenshot below.

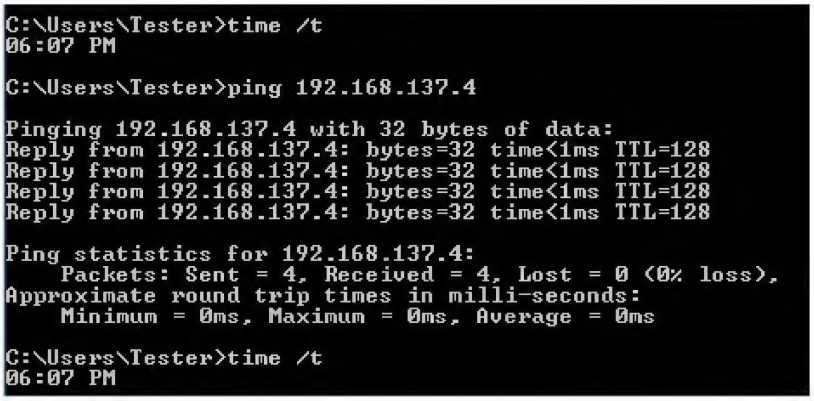


Figure 111. Screenshot of ping from Computer A (192.168.137.4) to Computer B (172.16.3.5) indicating 0% packet loss, demonstrating that the security gateway forwarded the packets.

631. As demonstrated by the ping requests detailed above, the TippingPoint security gateway segment 1 receives packets associated with communication to and from Network B, which is

protected by said security gateway. Thus, the TippingPoint system has been demonstrated to satisfy all requirements of claim element 1b of the '213 Patent.

632. Furthermore, as demonstrated in detail below, HTTP requests contained in TCP/IP packets can also be received by the packet security gateway and can be forwarded or dropped.

633. Thus, Exponent has demonstrated that the TippingPoint IPS method includes receiving, by a packet security gateway (i.e. SEG 1) of the plurality of packet security gateways (i.e. SEG 1 and SEG 2), packets associated with a network protected by the packet security gateway.

634. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1b of the '213 Patent.

635. **Claim 1c: identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information;** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

636. To demonstrate the functionality of the TippingPoint IPS, as required by this claim element, an alternative test configuration setup with two computers on a test network was configured, as shown in Figure 112.

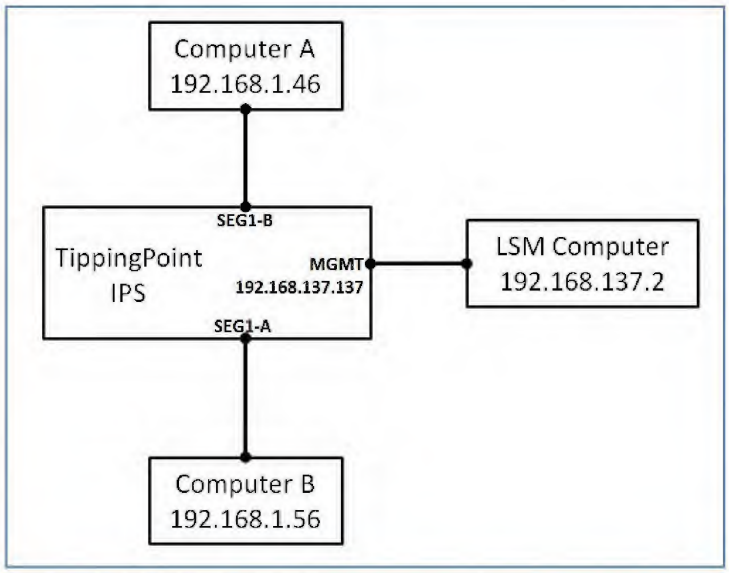


Figure 112. Network map of test network illustrating connectivity of TippingPoint IPS, Computer A, Computer B, and LSM Computer.

637. The TippingPoint system security gateway segment (SEG 1) is located at an interface between Network A, which contains Computer A, and Network B, which contains Computer B. The packet security gateway segment 1 receives packets associated with communication to and from Network B, which is protected by said security gateway. In this test network, one computer was configured to operate as an HTTP client and one to operate as an HTTP server. Computer B, at network IP address 192.168.1.56, was configured to operate as an HTTP server.[129] Computer A, at network IP address 192.168.1.46, was used to make HTTP GET requests to attempt to access the URL path "/etc/passwd" on the HTTP server. That is, Computer A was configured to operate as an HTTP client.

638. The '213 Patent indicates that "[i]n some embodiments, identifying the packets comprising the application-layer packet-header information may include the packet security

[129] We used a python programming language via a python language interpreter and standard python module called "http.server" to run an HTTP server on Computer B. For additional information, see https://docs.python/org (generally) as well as https://docs.python.org/2/library/simplehttpserver.html and https://docs.python.org/3/library/http.server.html.

gateway determining that the packets are among the HTTP packets identified by the rule(s) (e.g., the HTTP GET method call and/or the HTTP PUT method call may specify one or more URIs, and packet security gateway 112 may determine that the packet(s) originated from and/or are destined for a network address corresponding to the URI(s))." Thus, the packets containing the GET Method and the URL "http://192.168.1.46/etc/passwd" are identified by that application-layer packet-header information.

639. Initially, the "action" for the TippingPoint system's 0361 filter, which corresponds to the "HTTP: Protected File Access" threat, was configured to "Permit + Notify." While the "action" for this filter was configured to "Permit + Notify" this threat, a first packet, including an HTTP GET request for the URL path "/etc/passwd," was sent by Computer A to the IP address associated with Computer B. During this demonstration, the HTTP server on Computer B was configured to serve web pages on port 8000 rather than port 80.[130]

640. To send the HTTP GET request, Exponent used the program called "netcat." The "netcat" program is a well-known utility[131] for sending data using the TCP/IP protocol, which was used to send HTTP requests in this demonstration.[132] The netcat utility was used rather than a more complex web browser (e.g., Chrome or Internet Explorer) in order to enable more fine-grained control over the transmitted test packets.

641. A terminal window display from Computer A is shown in Figure 113. This figure shows (1) the use of netcat (the command line invocation of netcat is performed via the "nc" command) on Computer A to connect to port 8000 on Computer B (first line); (2) the HTTP GET request for the "etc/passwd" path (second line); (3) the HTTP response from the web server at Computer B indicating that the file was not found (remaining lines).

---

130 Port 8000 is the default port used by the python http server module.
131 See, for example, http://netcat.sourceforge.net/ and https://nmap.org/ncat/.
132 HTTP is an application layer protocol that typically runs on top of the lower-level TCP protocol.

```
exponent@adam-jumpkit:~$ nc 192.168.1.56 8000
GET /etc/passwd HTTP/1.1

HTTP/1.0 404 File not found
Server: SimpleHTTP/0.6 Python/3.4.2
Date: Wed, 30 May 2018 01:20:41 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Content-Length: 452

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 404</p>
        <p>Message: File not found.</p>
        <p>Error code explanation: 404 - Nothing matches the given URI.</p>
    </body>
</html>
```

Figure 113. **Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, the HTTP GET request for the "/etc/passwd" path, and the response from Computer B indicating that the "etc/passwd" file was not found by the server (thus it responds with a 404 error).**

642. Because the TippingPoint IPS was configured to "Permit + Notify" this threat, the HTTP GET request was allowed to pass from Computer A, through the TippingPoint IPS, and arrive at Computer B. The arrival of the HTTP GET request at Computer B is illustrated in Figure 114, which shows that the GET request for the path "/etc/passwd" invokes an HTTP code 404 response from the HTTP server. The 404 response also appears back at the HTTP client, as Figure 113 shows. The response is a code 404 because the file "/etc/passwd" is not available on the HTTP server.

```
C:\Users\Tester\Desktop\web>python -m http.server
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.46 - - [29/May/2018 18:20:41] code 404, message File not found
192.168.1.46 - - [29/May/2018 18:20:41] "GET /etc/passwd HTTP/1.1" 404 -
```

Figure 114. **Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server has sent back an HTTP code 404 in response to the GET request for "/etc/passwd."**

643. As Figure 115 illustrates, the "Alert Log" on the TippingPoint LSM GUI shows[133] that the first packet was detected and allowed to continue to its intended destination. More specifically, Figure 115 shows that the HTTP attack packet associated with the 0361 filter was received from the source 192.168.1.46 (Computer A) and allowed to continue to destination 192.168.1.56 (Computer B).



Figure 115. Screenshot from the TippingPoint LSM GUI showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was allowed.

644. Thus, it has been demonstrated that the TippingPoint IPS method includes the packet security gateway identifying "one or more packets comprising the application-layer packet-header information," on a packet-by-packet basis, "from amongst the packets associated with the network protected by the packet security gateway."

645. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1c of the '213 Patent.

646. **Claim 1d: performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

---

[133] See "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005) section "Alert Log" starting on p. 115.

647. As demonstrated in the analysis of claim element 1c above, the TippingPoint system can log attack packets based on identifying application-layer packet-header information. The TippingPoint system can perform other packet transformation functions as well, as detailed above in relation to claim element 1a. For example, the packets can also be blocked.

648. To demonstrate the functionality of the TippingPoint system, as required by this claim element, the TippingPoint IPS was configured to "Block + Notify" the same HTTP threat corresponding to the 0361 filter, as shown in Figure 116. A second packet, which included an HTTP GET request for the URL path "/etc/passwd," was then sent by Computer A to the IP address associated with Computer B.

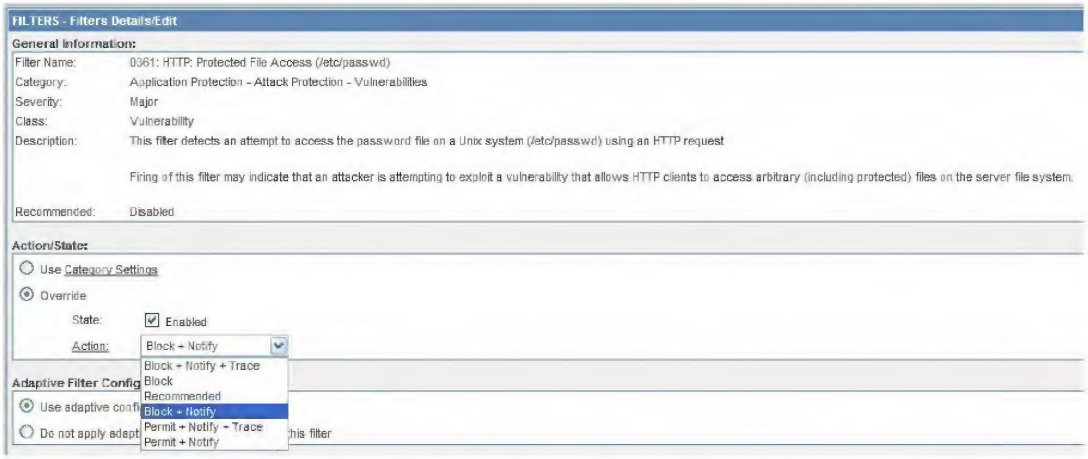


Figure 116. Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from "Permit + Notify" to "Block + Notify."

649. Figure 117 shows a terminal window display from Computer A. Specifically, it shows (1) the use of netcat (the command line invocation of netcat is performed via the "nc" command) on Computer A to connect to port 8000 on Computer B (first line); (2) the HTTP GET request for the "etc/passwd" path (second line); and (3) the absence of any HTTP response from the web server at Computer B and subsequent shutdown of the HTTP client using the "Ctrl-C" keyboard combination to send the client process a kill signal.

CENTRIPETAL-CSCO 087747

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 247

```
exponent@adam-jumpkit:~$ nc 192.168.1.56 8000
GET /etc/passwd HTTP/1.1

^C
```

Figure 117. **Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, and the HTTP GET request for the "/etc/passwd" path. It also illustrates that no response was received from Computer B (because Computer B never received the request).**

650. Figure 118 illustrates the "Block Log" on the LSM GUI, which shows[134] that the second packet was detected and blocked by the TippingPoint IPS packet filter. More specifically, Figure 118 shows that the HTTP attack packet associated with the 0361 filter was received from source 192.168.1.46 (Computer A) and blocked from continuing to destination 192.168.1.56 (Computer B).

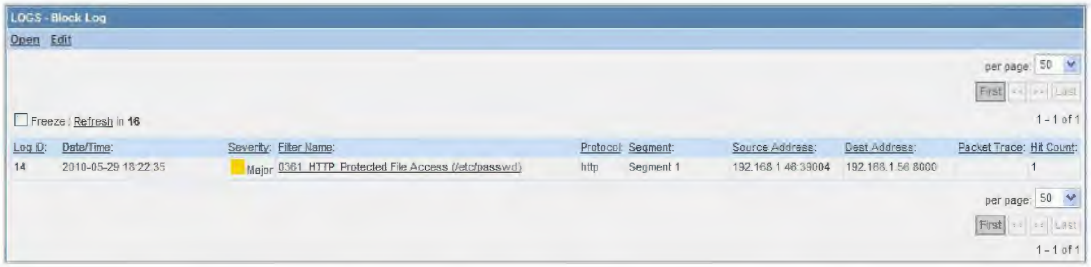


Figure 118. Screenshot from the TippingPoint LSM GUI, showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was blocked.

651. Because the TippingPoint IPS was configured to "Block + Notify" this HTTP file access threat prior to the arrival of the second packet, the HTTP GET request was *not* allowed to pass from Computer A through the TippingPoint IPS. Therefore, this packet never arrived at Computer B. The lack of arrival (i.e., being blocked) is evident in Figure 119, which shows the same text as Figure 114. The figure also exhibits additional whitespace, indicating that the request was not received; had the request been received, there would be a second code

134 See "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005) section "Block Log" starting on p. 116.

404 response logged to the terminal windows as well as a second GET request logged to the terminal window; however, no such log lines were displayed.

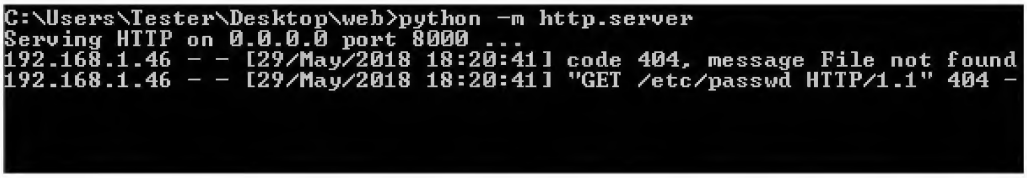


Figure 119. Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server did not send back any additional response because it did not receive the second packet. (The response shown in the figure is the response to the first packet.)

652. Hence, it has been demonstrated that the TippingPoint IPS method includes the packet security gateway performing a packet transformation function on the packets comprising the application-layer packet-header information, thus satisfying the requirements of claim element 1d.

653. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1d of the '213 Patent.

654. **Claim 1e: identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

655. As demonstrated above in relation to my analysis of claim elements 1a, 1c, and 1d, the packet transformation function may include not only blocking and/or forwarding, but also packet digest logging functionality. See, for example, Figure 118, which shows the "Block Log" for the blocked packet. The Block Log contains a subset of information for each of the packets comprising the application-layer packet-header information, e.g., source IP/port and

destination IP/port are shown in Figure 118, which is a subset of the packet information of the blocked application-layer packet.

656. Thus, for at least the same reasons as detailed above, it is my opinion that the TippingPoint system satisfies all requirements of claim element 1e.

657. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1e of the '213 Patent.

658. **Claim 1f: generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

659. As demonstrated above in relation to my analysis of claim elements 1a, 1c, and 1d, the packet transformation function performed by the packet security gateway includes not only blocking and/or forwarding, but also record generation functionality. See, for example, Figure 118, which shows the "Block Log" for the blocked packet. The row of data shown in the Block Log for the blocked packet is a record that was generated for logging the blocked attack event

660. Thus, for at least the same reasons as detailed above, it is my opinion that the TippingPoint system satisfies all requirements of claim element 1f.

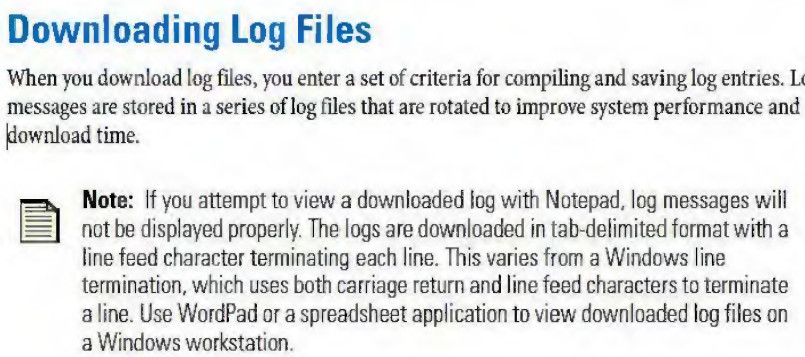
661. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1f of the '213 Patent.

662. **Claim 1g: reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the**

packet digest logging function in accordance with a logging system standard; and As detailed below, the TippingPoint system satisfies all requirements of this claim element.

663. As demonstrated above in relation to my analysis for Claim 1, the TippingPoint IPS logs attack packets "comprising application-layer packet-header information." For example, the "Block Log" shown in Figure 118 will contain a row of data for each blocked attack packet. This data constitutes a "subset of information specified by the packet digest logging function in accordance with a logging system standard." I understand that the parties have agreed that the term "logging system standard" is to be construed as "a standard for logging information," and I have applied this construction throughout my analysis.

664. The TippingPoint IPS logs can be managed using the LSM GUI.[135] These log entries can be downloaded and saved.[136] According to the TippingPoint documentation, downloaded log entries can be *reformatted* as tab-delimited lines of data terminated with a line-feed character, as shown in Figure 120, which displays a screen capture from the LSM User's Guide.[137]



Downloading Log Files

When you download log files, you enter a set of criteria for compiling and saving log entries. Log messages are stored in a series of log files that are rotated to improve system performance and download time.

Note: If you attempt to view a downloaded log with Notepad, log messages will not be displayed properly. The logs are downloaded in tab-delimited format with a line feed character terminating each line. This varies from a Windows line termination, which uses both carriage return and line feed characters to terminate a line. Use WordPad or a spreadsheet application to view downloaded log files on a Windows workstation.

Figure 120. Screen Capture from LSM User Manual indicating that logs can be downloaded in tab-separated format.

[135] See, "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 113, section "Log."
[136] Ibid, at page 122.
[137] Ibid

665. In addition, the TippingPoint system allows for IPS logs to be downloaded as .csv files, which are reformatted versions of the log files. To demonstrate this Exponent downloaded the IPS logs associated with our TippingPoint system tests used for the demonstrations relating to previous elements of Claim 1 of the '213 Patent, as depicted in Figure 121.



Figure 121. A log of packets sent from Computer B to Computer A, including the option to download (in the Edit menu).

666. As seen in Figure 122, the LSM GUI includes an option to download these logs as .csv files, which are reformatted versions of the log files. Furthermore, a POSITA would recognize that .csv files are a widely used standard for logging information, and thus satisfy the agreed upon construction for "logging system standard."

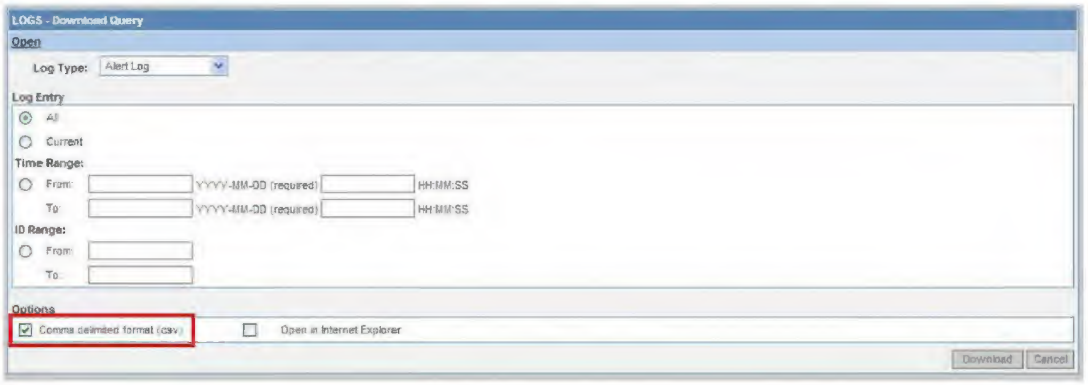
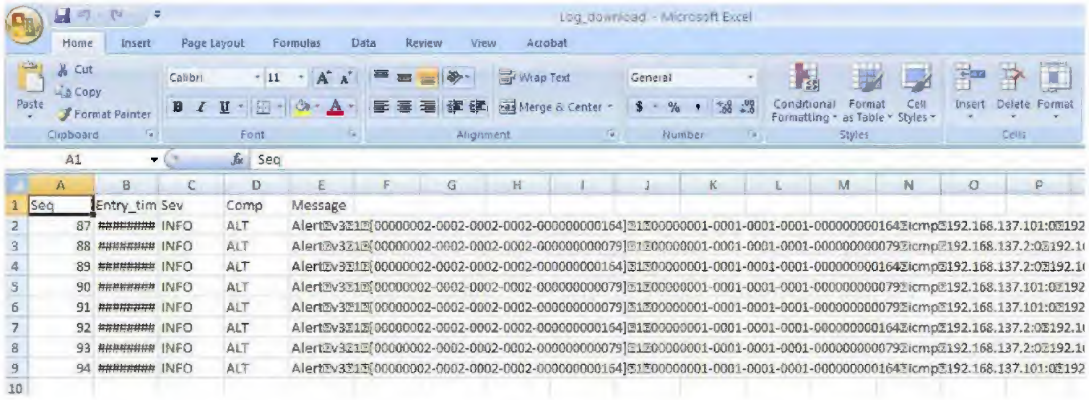


Figure 122. Download options, including specific time ranges and an option to download a .csv formatted log.

667. And finally, the downloaded .csv files can be opened in Microsoft Excel to view their contents, as shown in Figure 123.



Seq	Entry_tim	Sev	Comp	Message
87	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000164]⊡1⊡00000001-0001-0001-0001-000000000164⊡icmp⊡192.168.137.101:0⊡192
88	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000079]⊡1⊡00000001-0001-0001-0001-000000000079⊡icmp⊡192.168.137.2:0⊡192.1
89	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000164]⊡1⊡00000001-0001-0001-0001-000000000164⊡icmp⊡192.168.137.2:0⊡192.1
90	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000079]⊡1⊡00000001-0001-0001-0001-000000000079⊡icmp⊡192.168.137.101:0⊡192
91	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000079]⊡1⊡00000001-0001-0001-0001-000000000079⊡icmp⊡192.168.137.101:0⊡192
92	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000164]⊡1⊡00000001-0001-0001-0001-000000000164⊡icmp⊡192.168.137.2:0⊡192.1
93	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000079]⊡1⊡00000001-0001-0001-0001-000000000079⊡icmp⊡192.168.137.2:0⊡192.1
94	########	INFO	ALT	Alert⊡v3⊡1⊡[00000002-0002-0002-0002-000000000164]⊡1⊡00000001-0001-0001-0001-000000000164⊡icmp⊡192.168.137.101:0⊡192

Figure 123. Contents of downloaded .csv formatted log file

668. Thus, for at least the same reasons as detailed above, it is my opinion that the TippingPoint system satisfies all requirements of claim element 1g.

669. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1g of the '213 Patent.

670. **Claim 1h: routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.** As detailed below, the TippingPoint system satisfies all requirements of this claim element.

671. As demonstrated above in relation to my analysis of claim element 1a, the TippingPoint IPS can implement filters with an "action" that can be configured to "Block+Notify+Trace" the packet corresponding to the HTTP protected file access network threat. The "Trace" functionality records a copy of the attack packet to a log server, i.e., the packet is routed to a

monitoring device. For example, when this functionality is enabled the "Block Log" will show an entry in the "Packet Trace" column, as seen in Figure 124.



Figure 124. Screenshot from the LSM GUI showing the Block Log, which lists packets that were not forwarded to their intended destination.

672. By downloading the packet trace (see "Packet Trace" column in Figure 124) and opening it in Wireshark,[138] Exponent was able to view the contents of the packet during the demonstration (see Figure 125).

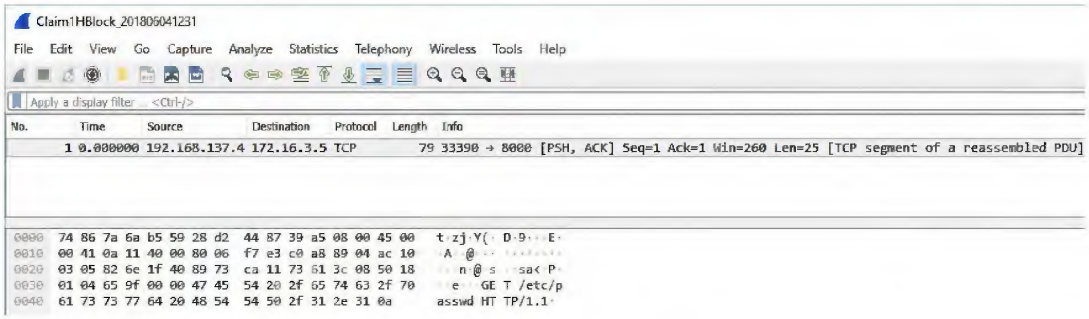


Figure 125. Packet information logged by the TippingPoint system. For example, the ASCII characters "GET /etc/passwd HTTP/1.1" can be seen in the lower right section of this figure.

673. The application-layer packet information can be seen in Figure 125. For example, the string "GET /etc/passwd" is seen in the lower right of the figure.

674. Thus, the TippingPoint IPS includes the method in which the packet security gateway can filter network traffic on a packet-by-packet basis, and perform a packet transformation on packets corresponding to the application-layer packet-header information, wherein said

[138] Wireshark is a network analysis computer program. See, for example, https://www.wireshark.org.

CENTRIPETAL-CSCO 087754

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 254

packets are routed to a monitoring device. Thus, for at least the reasons detailed above, it is my opinion that the TippingPoint system satisfies all requirements of claim element 1h.

675. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates claim element 1h of the '213 Patent.

676. Consequently, for at least the reasons above, it is my opinion that each and every element of Claim 1 of the '213 Patent is anticipated by the TippingPoint system.

3. CLAIM 3

677. **The method of claim 1, wherein the at least one rule indicates performing a deny packet transformation function on the packets comprising the application-layer packet-header information, and wherein the performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information.** As detailed below, the TippingPoint system satisfies all requirements of this claim.

678. As demonstrated above in relation to my analysis of claim elements 1a and 1d, the TippingPoint filter corresponding to the application-layer packet-header information is configured to "Block+Notify+Trace," in claim element 1a, and "Block+Notify," in claim element 1d. These configurations both block the attack packet, which constitutes a "deny packet transformation function." In both cases, the packet is dropped by the packet security gateway (i.e. SEG 1) rather than being allowed to continue to its destination.

679. Thus, for at least the reasons detailed above, it is my opinion that the TippingPoint system satisfies all requirements of Claim 3.

680. Therefore, for at least the reasons given above, it is my opinion that the TippingPoint system anticipates Claim 3 of the '213 Patent.

C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF CHECK POINT R75

681. The Check Point R75 security gateway (SG) product[139] performs the functionality of a packet security gateway, and the Check Point R75 security management server (SMS) product[140] performs the functionality of security policy management server. An illustration of how the R75 SG and R75 SMS fit into a typical network architecture is shown in Figure 126.

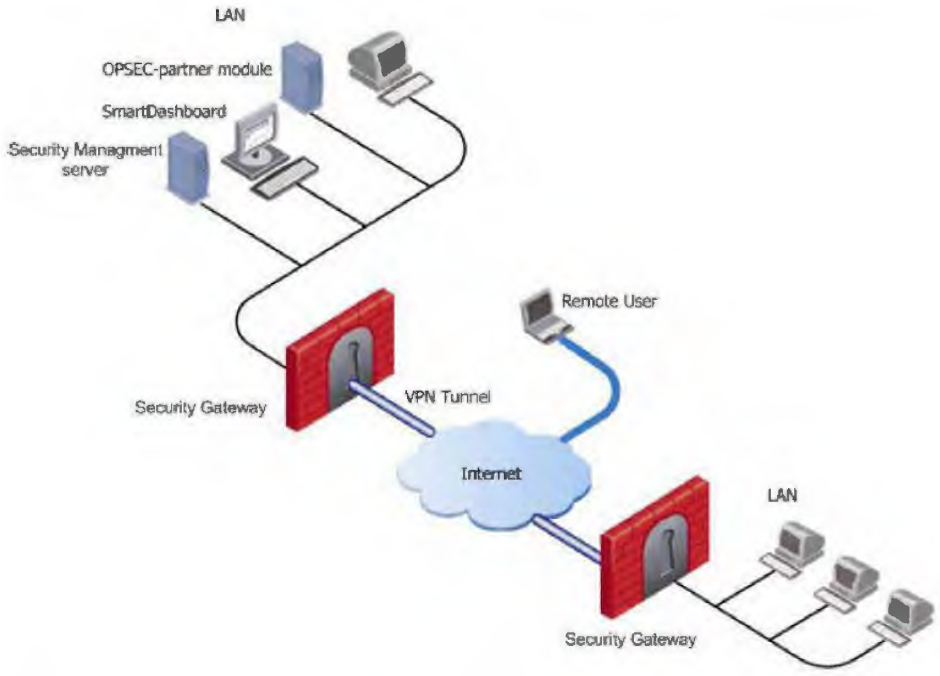


Figure 126. Illustration of a typical deployment consisting of two security gateways and a security management server (configurable using the "SmartDashboard" GUI).[141]

682. The Check Point R75 system was commercially available to purchase before the priority date of the '213 Patent, and I have been informed by counsel that the Check Point R75 system constitutes prior art to this patent.

---

139 See "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).
140 See "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).
141 See p. 10, "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).

683. For at least the reasons detailed below, it is my opinion that the Check Point R75 system enabled a person of ordinary skill in the art to practice each and every element of Claims 1 and 3 of the '213 Patent, and thus the Check Point R75 system anticipates these claims.

1. TEST CONFIGURATION WITH CHECK POINT R75

684. Exponent procured the Check Point R75 SMS product and installed it on a 32-bit PC-compatible Dell Latitude E6400 computer using the "Check_Point_R75.Splat.iso" DVD ISO image.[142]

685. Exponent also procured the Check Point R75 SG product and installed it on two 32-bit PC-compatible Dell PowerEdge 1750 computers using the "Check_Point_R75.Splat.iso" DVD ISO image.

686. The SMS and SGs were installed in a "Distributed Deployment" configuration (see Figure 126) wherein the SMS is installed on a different machine than the SGs.

687. Figure 127 shows the physical layout of the hardware, including the two security gateways, the security management server, the SmartDashboard interface, three switches, and three computers for sending and receiving traffic.



Figure 127. Photograph of test network used as part of the claim analysis that shows a hardware installation of two security gateways (SG 1 and SG 2, labelled as "gw1"

[142] According to the Check Point website, DVD installation material was available in December 2010 (see https://supportcenter.Check Point.com/supportcenter/) and the installation procedure for the Firewall and Security Management Server is documented in the "R75 Installation and Upgrade Guide."

CENTRIPETAL-CSCO 087757

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 257

and "gw2" in the figure, respectively), one security management server (SMS) with its associated SmartDashboard graphical user interface (GUI).

688. The test network shown in Figure 127 includes three subnetworks (subnets). The first subnet is called "Network A" and includes "Computer A" at IP address 172.16.3.3. The second subnet is called "Network B" and includes "Computer B' at IP address 192.168.1.100. Network A and Network B are connected by an R75 SG, which we refer to as "Security Gateway 1" or "SG 1." This security gateway is also referred to as "gw1" in the SmartDashboard GUI and is labeled as such in Figure 127.

689. The third subnet is called "Network C" and includes "Computer C' at IP address 10.0.42.16. This security gateway is also referred to as "gw2" in the SmartDashboard GUI and is labeled as such in Figure 127.

690. Figure 128 shows the schematic layout of the test network used as part of the claim analysis herein. The IP addresses of each host are assigned as shown in the figure. Network B includes the R75 SMS (the security policy management server) along with another computer called "Computer B." Security Gateway 1 protects Network A from Network B. Security Gateway 2 protects Network B from Network C.

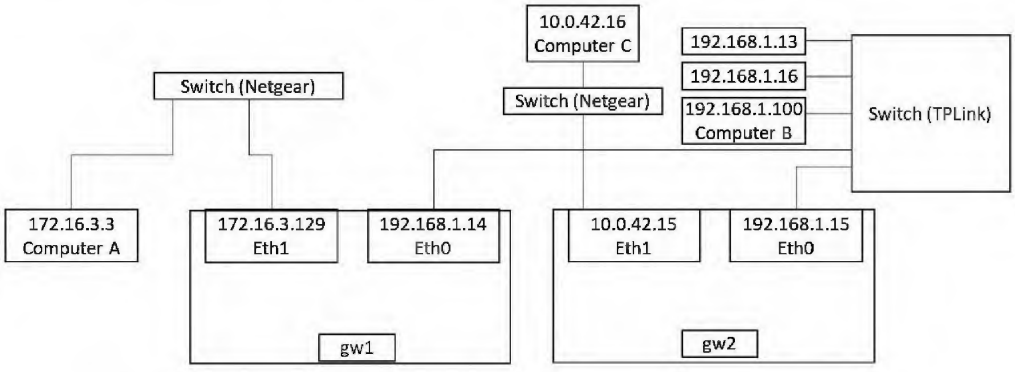


Figure 128. Schematic of test network used in claim analysis (see Figure 127), including the static IP addresses of each element.

CENTRIPETAL-CSCO 087758

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 258

2. CLAIM 1

691. **Claim 1a: A method comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;** As detailed below, the Check Point R75 system satisfies all requirements of this claim.

692. The '213 Patent states that "[a]s used herein, a security policy management server includes any computing device configured to communicate a dynamic security policy to a packet security gateway."[143] I understand that in relation to the '213 Patent the parties have agreed that the term "security policy management server" is to be construed as "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway," in accord with the Joint Claim Construction Statement.[144] For my analysis I have considered the agreed upon construction of the term "security policy management server," as well as the description of this term within the '213 Patent specification, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. In any event, the Check Point R75 system comprises a security policy management server for at least the reasons detailed below.

693. The Check Point R75 system includes the Check Point R75 security management server (SMS). According to the Check Point R75 Security Management Server Administration Guide, the "*Security Management server* is the component that manages the database and

[143] '213 Patent, at 4:53-55.
[144] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL)).

CENTRIPETAL-CSCO 087759

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 259

policies, and downloads policies to gateways."[145] This guide also states that "[t]he Security Management server manages the gateways and allows remote users to connect securely to the corporate network." [146] It goes on to state that "SmartDashboard may be installed on the Security Management server or on any other machine." SmartDashboard is the "set of GUI applications used to manage different aspects of the corporate network" referred to as "SmartConsole," which is "used to create, edit and install policies," and allows for the management of objects that "represent actual network components such as gateways, servers and networks."[147] Thus, the Check Point R75 system includes a graphical user interface (GUI) with which dynamic security policies may be managed and communicated to the Check Point R75 security gateways. Therefore, the Check Point R75 system includes "a server configured to manage policies and communicate a dynamic security policy to a packet security gateway," as required by the claim construction of "security policy management server." Moreover, although I have applied the agreed upon claim constructions throughout my analysis, the Check Point R75 system also satisfies the definition for "security policy management server" stated within the '213 Patent, at least because the laptop running the security management server (SMS) with its associated SmartDashboard graphical user interface (GUI) constitutes a "computing device configured to communicate a dynamic security policy to a packet security gateway."

694. I understand there is a dispute regarding the construction of the term "dynamic security policy," in relation to the '213 Patent. More specifically, Plaintiff has proposed that this term be construed as "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets," while Defendants have proposed that this

[145] See p.11"Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).
[146] See p.10"Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).
[147] See p.11"Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).

term be construed as "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria".[148] According the '213 Patent specification, "[a] dynamic security policy includes any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria."[149] I have considered both proposed constructions in my analysis, in addition to the description of this term within the '213 Patent specification, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R75 system satisfies all requirements of this claim element, for at least the reasons detailed herein.

695. The Check Point R75 documentation explains that "[t]he Security Management Server enables administrators to enforce security policies," and that this is accomplished by administrators defining a security policy Rule Base. As stated in the Check Point R75 documentation[150] "[a] Security Policy consists of an ordered set of rules, collectively known as the Rule Base…The Security Gateway inspects packets and applies rules in a sequential manner. When a Security Gateway receives a packet from a connection, it inspects the packet and applies the first rule in the Rule Base, then the second rule and so on."[151] Thus, Check Point R75 system's Security Policies are "dynamic security policies."

---

[148] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.
[149] '213 Patent, Column 4, Lines 58–63.
[150] See pp. 9–11, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).
[151] See pp. 11, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

696. The '213 Patent states that "[a]s used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation on the packets."[152] I understand, however, that in relation to the '213 Patent, the parties have agreed that the term "packet security gateway" is to be construed as "a gateway computer configured to receive packets and perform a packet transformation function on the packets."[153] I have considered both the agreed upon construction as well as the description within the patent specification throughout my analysis, and regardless of which construction is applied, it is my opinion that the Check Point R75 system includes "a plurality of packet security gateways," and thus satisfies this claim requirement for at least the reasons below.

697. The Check Point R75 system includes two separate security gateways (Check Point R75 SGs), which are labeled "gw1" and "gw2" in Figure 127, that act as two separate packet security gateways where each security gateway can be programmed independently to follow its own set of rules via the Check Point R75 SMS. For example, as discussed in relation to Figure 127 and Figure 128, each security gateway receives packets traveling between networks, and then applies an ordered set of rules to these packets. More specifically, in Exponent's test setup described above, gw1 is located at the boundary between Network A and Network B, and receives all packets that pass between these two networks. Upon receiving packets, a computer within the Check Point R75 security gateway applies rules according to the currently applied security policy. Thus, the Check Point R75 system includes "a gateway computer configured to receive packets" as required by the agreed upon construction for "packet security gateway." The Check Point R75 system also satisfies the requirement of including "a plurality of packet security gateways" in accord with the

[152] '213 Patent, at 4:48-50.
[153] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.

description of a "packet security gateway" stated within the '213 Patent, at least because the laptop running the Check Point R75 SG constitutes a "computing device configured to receive packets and perform a packet transformation on the packets."

698. Furthermore, the check Point R75 SGs are each "associated with the security policy management server" at least because the dynamic security policies, and associated rules, can be installed on the selected gateways using the security management server,[154] and said policies, applied by gw1 and gw2, are configurable using the SmartDashboard installed on the Check Point R75 SMS.

699. I also understand that there was a dispute regarding the construction of the term "packet transformation function." More specifically, in relation to the '213 Patent, Plaintiffs proposed that this term be construed as "function that transforms packets from one state to another" while Defendants proposed "an operation performed on a packet specified by the dynamic security policy, such as forward or drop."[155] I have considered both proposed constructions in my analysis, as well as the example embodiment of packet transformations described within the '213 Patent specification, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R75 system satisfies the requirements for this term for at least the reasons discussed herein.

700. Plaintiff's proposed construction of "packet transformation function" requires a function that "transforms one or more packets from one state to another." Although Plaintiff's have not provided an explicit definition for transforming "from one state to another," the intrinsic

---

[154] See, generally, pp. 28–29, "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010); see also p. 9 "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010): "Granular security policy control is possible by applying specific rules to specific gateways."

[155] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

evidence cited to by Plaintiff in support of their proposed construction includes example embodiments in which packets are forwarded or dropped depending upon parameters of the packet such as the origination IP address. Thus, under Plaintiff's proposed construction, forwarding or dropping of packets constitutes transforming a packet from one state to another, and hence forwarding or dropping satisfy Plaintiff's construction of "packet transformation function." Similarly, Defendants' proposed construction for "packet transformation function" explicitly includes the operations "forward or drop," and hence forwarding or dropping also satisfy Defendant's proposed construction for this term. As detailed below in relation to other claim elements, the Check Point R75 can perform a variety of functions upon the received packets, depending upon the rules within the current policy and parameters of the received packets, including but not limited to: forwarding packets to their intended address; forwarding packets to an address other than their intended address; dropping packets; logging or otherwise monitoring packets. Therefore, the Check Point R75 system satisfies both parties' proposed construction for "packet transformation function."

701. Amongst example embodiments provided by the '213 Patent specification, "packet transformation functions," specified by the dynamic security policy, include forwarding, dropping, logging, or routing packets to a network address different from a packet's destination network address (i.e. rerouting) (*see* '213 Patent, col 2:36-59 and col 11:45-48).

702. As detailed below, the Check Point R75 system can perform a variety of functions upon the received packets, depending upon the rules within the current policy and parameters of the received packets, including but not limited to: forwarding packets to their intended address; forwarding packets to an address other than their intended address; dropping

packets; logging or otherwise monitoring packets. Therefore, the Check Point R75 satisfies all constructions for "packet transformation function."

703. Although the Check Point R75 system is capable of performing a variety of different "packet transformation functions," in accord with the various constructions of said term, the limitations of claim element 1a specifically requires that the packet transformation function "compris[e] a packet digest logging function to be performed on packets comprising the application-layer packet-header information." The Check Point R75 system operates on packet at a variety of different levels in the Internet protocol stack, including the "application layer." I understand, that the parties have agreed that the term "packet digest logging function" is to be construed as "a function that identifies a subset of information for a packet and generates a record," and that the term "application-layer packet-header information" is to be construed as "information in the header of a packet that corresponds to the application-layer." These are consistent with the plain and ordinary meaning of packet-header information, which is the portion of a packet that precedes its body and contains addressing and other data that is required for it to reach its destination; and also with the '213 Patent specification, which includes a variety of examples of "application-layer packet-header information," stating "[f]or example, application-layer hypertext transfer protocol (HTTP) packets … may contain headers that specify methods and/or one or more uniform resource identifiers (URIs) for transferring resources (e.g. files) between client and servers" ('213 Patent, col 7:49-55). As described by the '213 Patent specification, a "packet digest logging function" is a type of packet transformation function, specified by a rule, that "when applied to a packet that matches such a rule, produces a digest version, or log, of the packet. This packet log (or digest) may contain selected packet information and/or system information"

('213 Patent, col 11:47-50). As noted above, and discussed in greater detail below, the Check Point R75 system can perform packet transformation functions that include packet logging. Thus, the Check Point R75 system can perform the requirements of this claim element in accordance with the agreed upon constructions and the '213 Patent specification, therefore satisfying the limitations of this claim element.

704. It is my understanding that no claim construction has been submitted for the term "rule," with respect to the '213 Patent, and thus the plain and ordinary meaning should be applied. However, it is also my understanding that there was a dispute regarding the construction of this term in the Joint Claim Construction Statement[156] with respect to the '205 and '077 Patents. While I have applied the plain and ordinary meaning to the term "rule" for the '213 Patent, because the '213, '205, and '077 Patents have similar specifications, with similar or identical terms in the claim language, and address similar subject matters at similar points in time as would be understood by a similar POSITA, I have also considered the respective claim constructions addressed in the Joint Claim Construction Statement while performing my analysis herein

705. I understand that, with respect to the '205 and '077 Patents, Plaintiff has proposed that this term be construed as "condition or set of conditions that when satisfied cause a specific action to occur," while Defendants have proposed that this term be construed as "(i) packet-identifying criteria and (ii) a function to be performed on the identified packets."[157] I have considered both proposed constructions in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of

[156] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))
[157] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

which construction is applied, the Check Point R75 system satisfies all requirements of this claim element, for at least the reasons detailed below.

706. As discussed in relation to this claim element, the Check Point R75 system is able to implement rules that specify a set of criteria for which packets should be forwarded, dropped, and/or logged. These rules satisfy both the proposed claim constructions. For example, these rules contain a "condition or set of conditions" based upon, for example, packet-header information associated with received packets, as discussed above, and cause "a specific action to occur" (e.g. forward or drop) when packets satisfy said condition or set of conditions: thus, Plaintiff's proposed construction is satisfied. Also, for these rules the packet-header information of received packets may be used as "packet-identifying criteria," and "a function" (e.g. forward or drop) is "performed on the identified packets": thus, Defendants' proposed construction is also satisfied.

707. Using the test setup described above, Exponent has demonstrated that the Check Point R75 SGs receive dynamic security policies from the Check Point R75 SMS. Exponent installed dynamic security policies on the Check Point R75 system including both an explicit rule to accept incoming traffic (see Figure 129) as well as an implicit rule to block packets based on specific header information (see Figure 130).



Figure 129. Screenshot of Check Point SmartDashboard GUI showing dynamic security policy with an explicit firewall rule to allow packets.

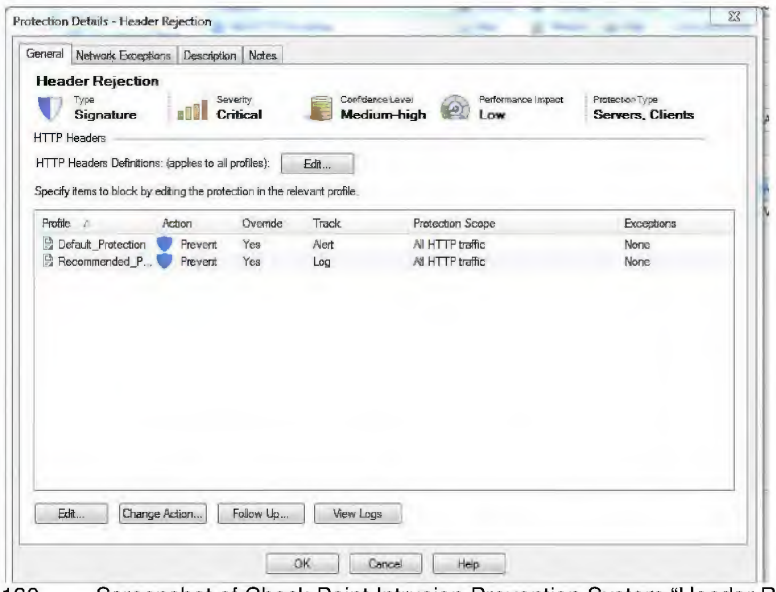


Figure 130. Screenshot of Check Point Intrusion Prevention System "Header Rejection" menu. The Action is currently set to "prevent"

708. The Check Point R75 system can be configured to detect and prevent network threats based on HTTP header values. For example, the Check Point R75 manual specifies that header rejection can be used to block, stating "MSN messenger communication that uses HTTP" based on HTTP request headers.[158] The R75 SMS GUI can be used to configure header rejection, as shown in Figure 130.

709. As stated above, the '213 Patent specifies that "application-layer hypertext transfer protocol (HTTP) packets, which transfer information between instances of web client applications (e.g., web browsers) and web server applications (e.g., named web sites such as www.examplewebsite.com), may contain headers that specify methods and/or one or more uniform resource identifiers (URIs) for transferring resources (e.g., files) between client and servers." Thus, the HTTP request headers comprise application-layer packet-header information.

[158] "CP_R75_Firewall_AdminGuide.pdf" at page 155.

710. Exponent configured the Check Point R75 "Header Rejection Pattern" to reject packets associated with HTTP request headers with header name "SampleRequestHeader" and header value "85" (see Figure 131 and Figure 132).

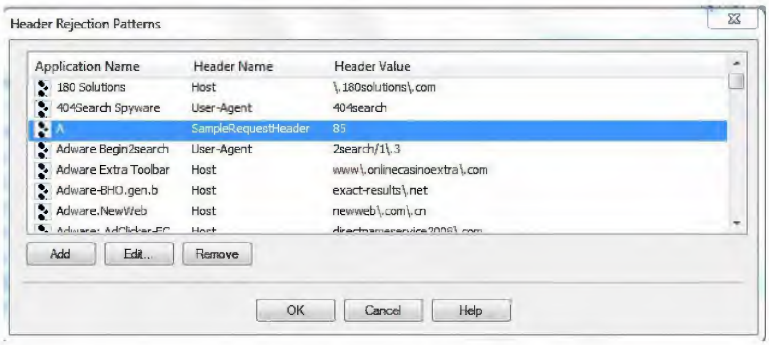


Figure 131. Screenshot of Check Point R75 list of headers that will be detected "Header Rejection," including the Exponent-configured rejection of traffic for custom headers with Header Name "SampleRequestHeader" and Header Value "85"

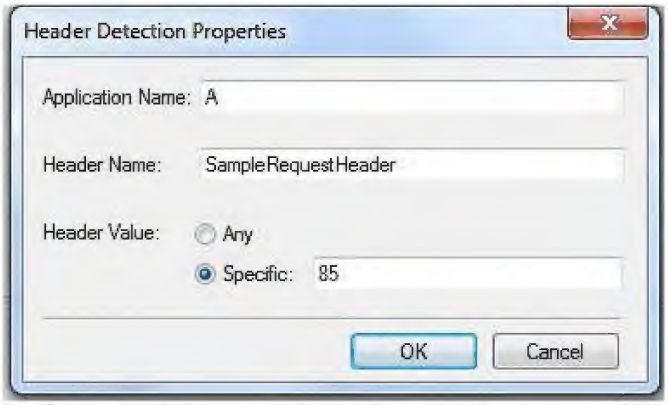


Figure 132. Screenshot of Header Detection properties for Header Name "SampleRequestHeader". The detection properties can be set to Any value or a specific value. Exponent set the relevant header value to 85 for this test.

711. Packets with rejected headers are logged and visible in the Check Point R75 SmartView Tracker. Figure 133 shows rejection of packets based on header content (e.g. under "Attack information").

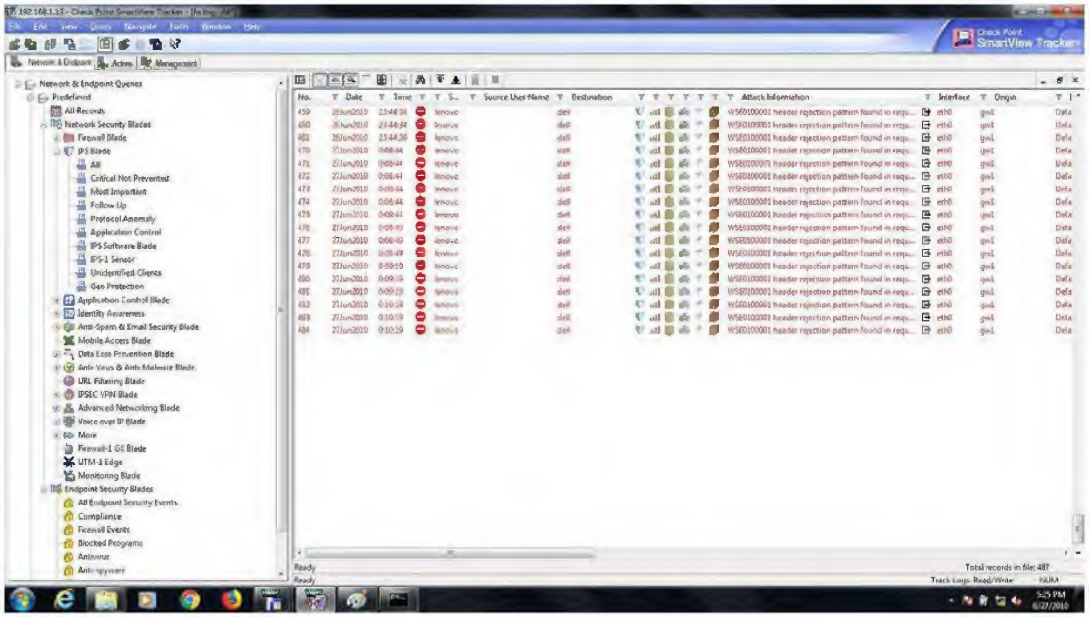


Figure 133. Screenshot of Check Point SmartView Tracker listing packets rejected based on configured dynamic security policies including rejection based on header content.

712. Thus, as explained above, the Check Point R75 system may contain a "plurality of packet security gateways associated with a security policy management server," wherein the packet security gateways (i.e. Check Point R75 SGs) receive "a dynamic security policy" from the Check Point R75 SMS, "that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information." As demonstrated above, the "Header Rejection" policy rule implements such a rule that can perform a packet digest logging function on packets comprising the application-layer packet-header information.

713. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1a of the '213 Patent.

714. **Claim 1b: receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;** As detailed below, the Check Point R75 system satisfies all requirements of this claim.

715. Using the Check Point R75 system shown in Figure 127, Exponent used a computer (Computer B at IP address 192.168.1.100) to send packet traffic to another computer (Computer A at IP address 172.16.3.3) protected by the packet security gateway. Packets were sent from Computer B to Computer A using a Google Chrome web browser with the "ModHeader" browser extension. [159] This allowed for the explicit configuration of the HTTP headers that were sent along with the web browser's HTTP requests. In this experiment, the web browser was configured to send HTTP requests including a HTTP header named "SampleRequestHeader" with header value "84," as shown in Figure 134 and Figure 135.

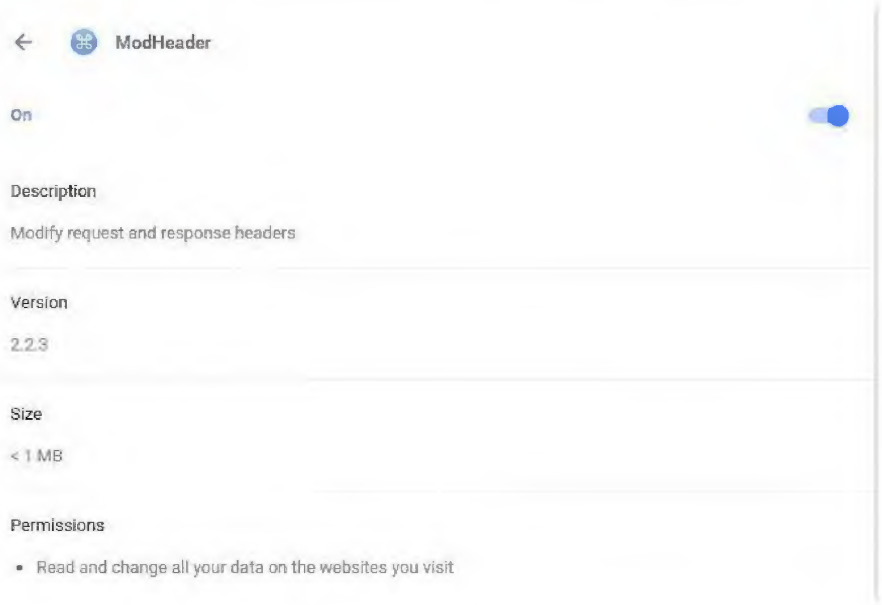


Figure 134. Screenshot of the Chrome browser "ModHeader" extension used to create custom request and response headers.

[159] https://addons.mozilla.org/en-US/firefox/addon/modheader-firefox/?src=hotness



Figure 135. Screenshot showing properties of the HTTP request header to be sent from Computer A.

716. Exponent set up an HTTP server on Computer A using the SimpleHTTPServer python module. An attempt was then made to load a sample HTML file on Computer B by browsing to 172.16.3:8000 (see Figure 136 and Figure 137).

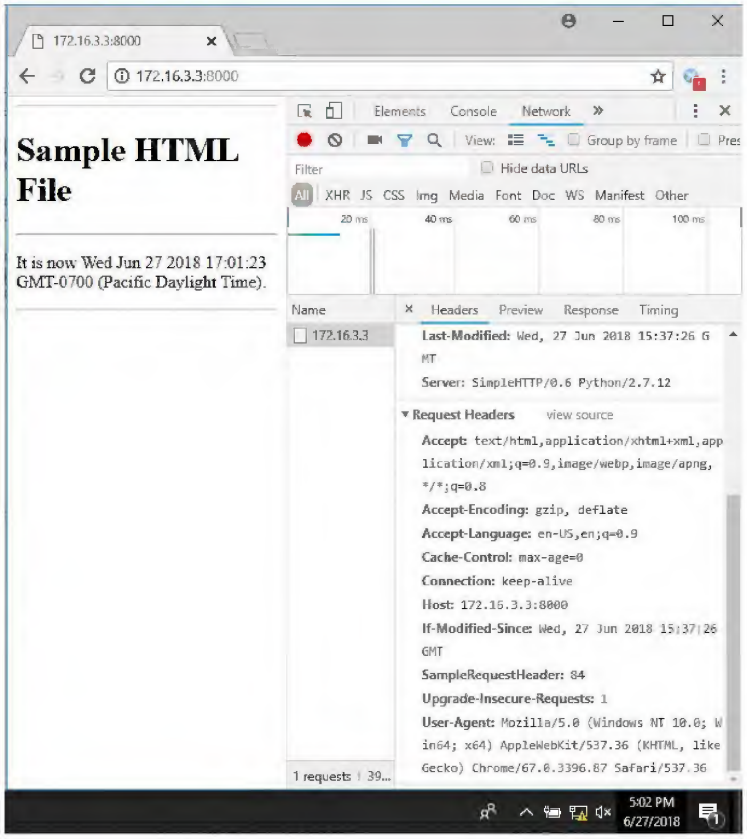


Figure 136. Screenshot from Computer B showing the sample HTML file was served from Computer A. Note that the packet header information shown on the right indicates the header name and number "SampleRequestHeader: 84" which are permitted by the security gate policies.



Figure 137. Screenshot from Computer A initiating the server and showing successful serving of the sample HTML file loaded by Computer B through the security packet gateway.

717. As shown in Figure 136 and Figure 137, the web browser at Computer B was allowed to connect to the web server at Computer A. The connection is allowed in this case because the SampleRequestHeader value is 84. That is, the request is allowed because the Check Point R75 policy rule is configured to block only headers with the value 85, not 84. If the header value is changed from 84 to 85 then the request will be blocked, as shown below.

718. While using the Check Point R75 system shown in Figure 127, Exponent reconfigured the web browser (see Figure 138) to make requests including the forbidden application-layer header content (SampleRequestHeader: 85) from Computer B to Computer A through the packet security gateway, gw1. The packet security gateway received the packet with the forbidden header content and blocked the transmission to Computer A, as can be seen in Figure 139 and Figure 140.

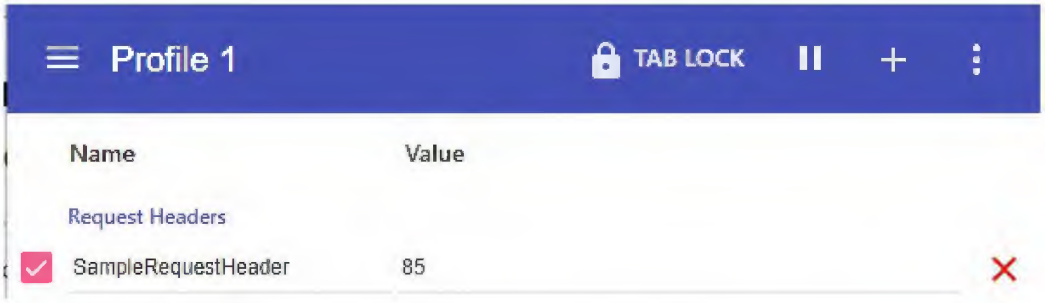


Figure 138. Screenshot showing properties of the HTTP request header to be sent from Computer B to Computer A.

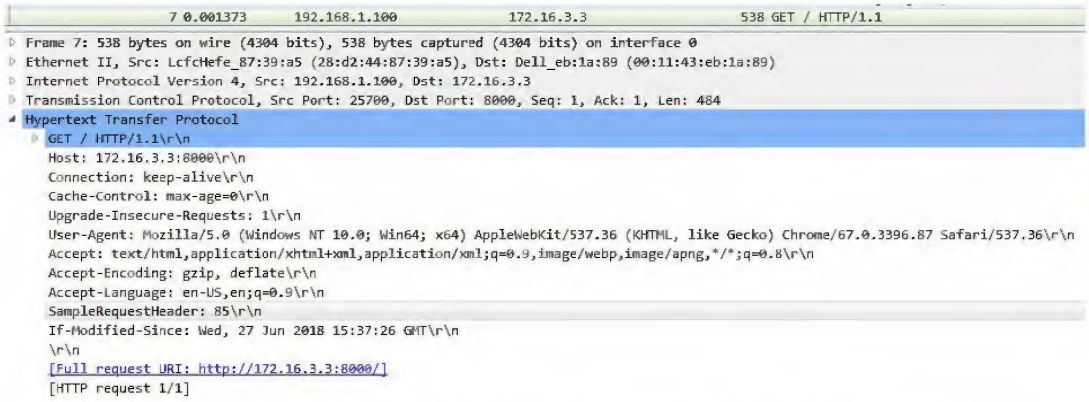


Figure 139. Wireshark screenshot showing the request from Computer B for the sample HTML file on Computer A that was blocked. The packet header information shown on indicates the header name and number "SampleRequestHeader: 85" which are the values Exponent set to be blocked by the R75 security gate policies.

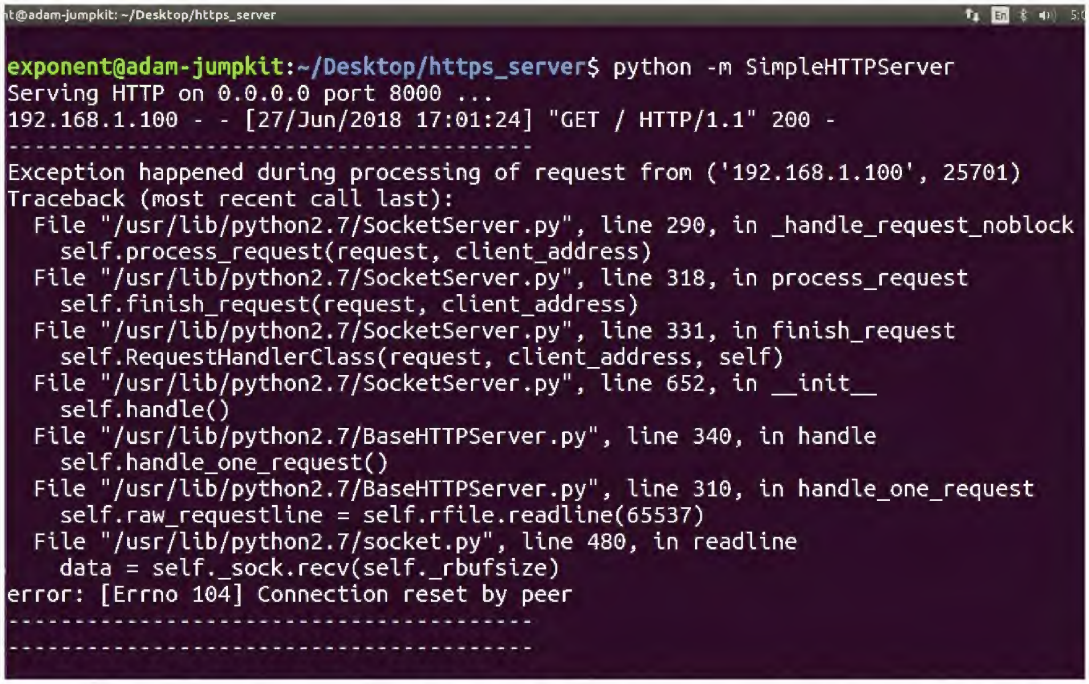


Figure 140. Screenshot from Computer A initiating the server and showing two attempts to serve the sample HTML file to Computer B. In the first attempt (above the first dotted line) the header value is set to 84 and the packet is received by Computer B. In the second attempt (below first dotted line) the header value is set to 85 and Check Point R75 security gateway policies receive the packet and block transmission to Computer B.

719. As demonstrated by the web browser requests detailed above, the Check Point R75 security gateway 1 receives packets associated with communication to and from Network B, which is protected by said security gateway. Thus, Exponent has demonstrated that the Check Point R75 method includes receiving, by a packet security gateway (i.e. gw1) of the plurality of packet security gateways (i.e. gw1 and gw2), packets associated with a network protected by the packet security gateway, and thus the Check Point R75 system satisfies the requirements of claim element 1b of the '213 Patent.

720. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1b of the '213 Patent

721. **Claim 1c: identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information;** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

722. To demonstrate the functionality of the Check Point R75 system, as required by this claim element, Exponent sent packet traffic from Computer B to Computer A through the packet security gateway, gw1, using the Check Point R75 system configuration setup shown in Figure 127. The packets were received by the packet security gateway and either transmitted or blocked based on the application-layer packet-header information as shown above.

723. Figure 141 and Figure 142 show traffic and packet details for the non-excluded header information (header name/value pair SampleRequestHeader/84).

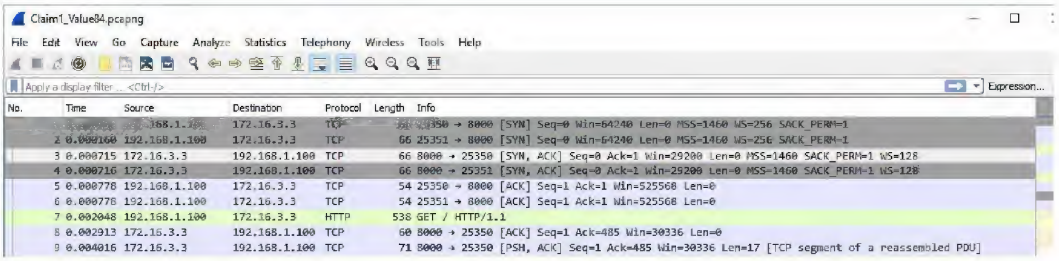


Figure 141. Screenshot of WireShark program showing traffic sent to and from Computer A (IP 172.16.3.3) and Computer B (IP 192.168.1.100). Packet number 7 was allowed to pass to Computer A through the packet security gateway based on the header information shown in Figure 142.

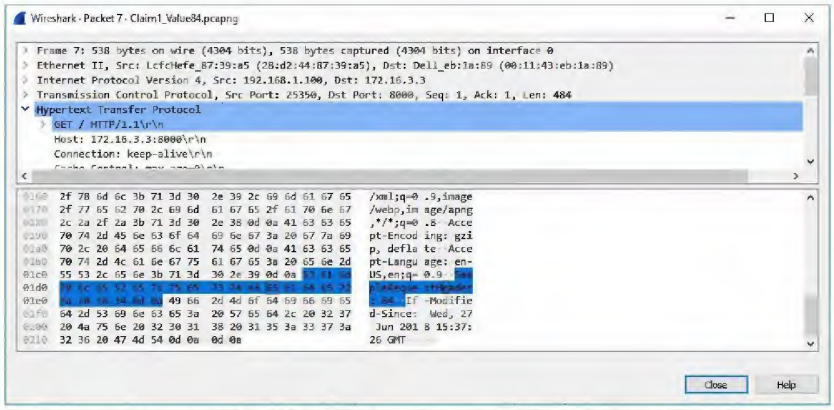


Figure 142. Screenshot of WireShark program with details of packet sent with non-excluded header content "SampleRequestHeader: 84," which is a non-excluded value.

724. Exponent also demonstrated that the Check Point R75 system not only evaluates packet traffic associated with the network protected by the packet security gateway, but it evaluates said traffic "on a packet-by-packet basis." For example, Figure 143 and Figure 144 provide evidence that the packet with application-layer header value 84 was allowed to pass, whereas packets with application-layer header value 85 are blocked.

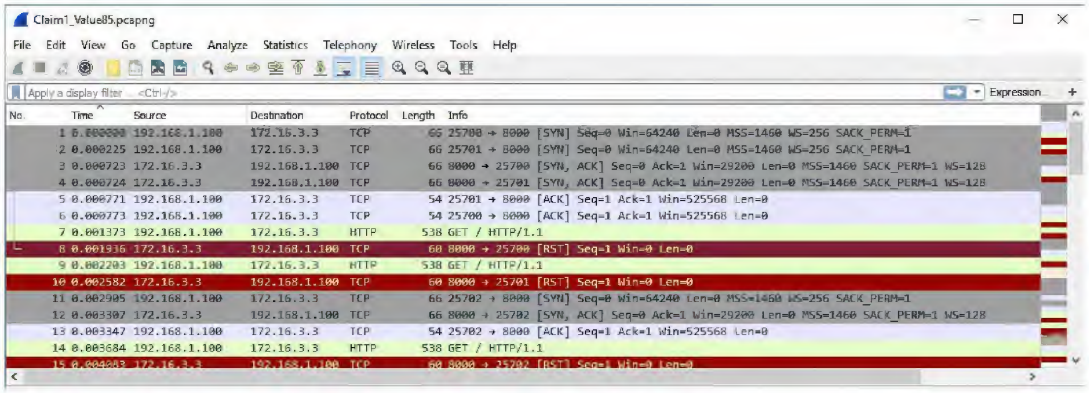


Figure 143. Screenshot of WireShark program showing traffic sent to/from Computer A (IP 172.16.3.3) and Computer B (IP 192.168.1.100).

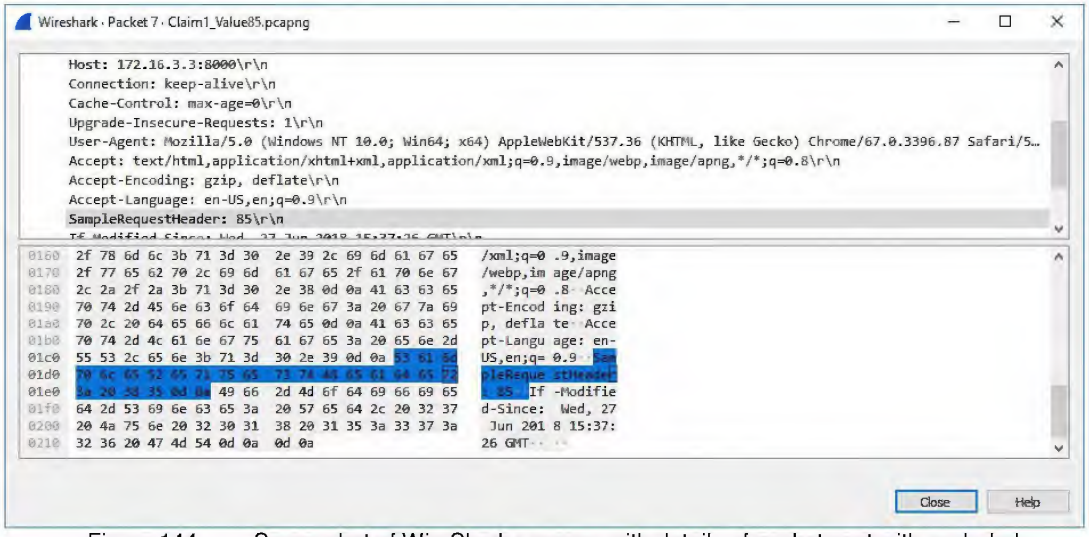


Figure 144. Screenshot of WireShark program with details of packet sent with excluded header content. The packet header is "SampleRequestHeader" and header value is "85", which is the excluded value.

725. Thus, it has been demonstrated that the Check Point R75 method includes the packet security gateway identifying "one or more packets comprising the application-layer packet-header information," "from amongst the packets associated with the network protected by the packet security gateway," and does so "on a packet-by-packet basis."

726. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1c of the '213 Patent

CENTRIPETAL-CSCO 087777

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 277

727. **Claim 1d: performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

728. As demonstrated above in relation to my analysis of claim elements 1c, the Check Point R75 system can drop or forward packets traffic based on a packet-by-packet analysis of the application-layer packet-header information. Dropping or forwarding constitute packet transformation functions.

729. Hence, it has been demonstrated that the Check Point R75 system includes the method whereby the packet security gateway performs a packet transformation function on the packets comprising the application-layer packet-header information, thus satisfies the requirements of claim element 1d.

Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1d of the '213 Patent

730. **Claim 1e: identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

731. As demonstrated above in relation to my analysis of Claim 1, the Check Point R75 system can block or accept (i.e. forward) packets in accord with the configuration of dynamic security policies based on application-layer packet-header information. A subset of

information about the blocked and allowed packets is logged by Check Point R75 and can be viewed in, for example, the Check Point SmartView Tracker, as shown in Figure 145.

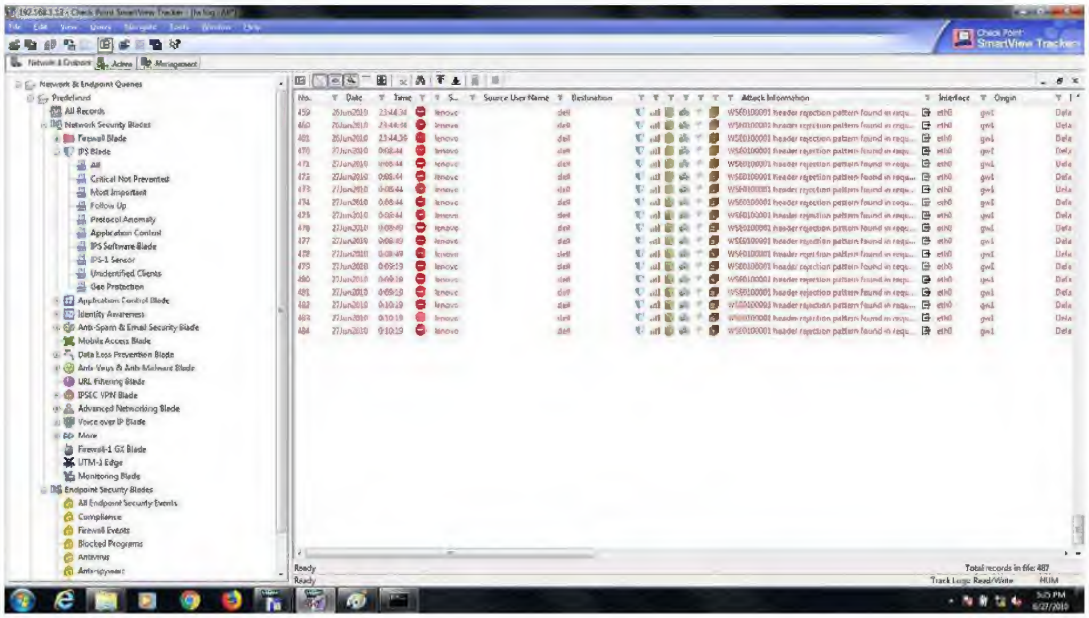


Figure 145. Screenshot of Check Point SmartView Tracker listing packets rejected based on configured dynamic security policies including rejection based on header content.

732. Thus, for at least the same reasons as detailed above, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 1e.

733. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1e of the '213 Patent.

734. **Claim 1f: generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and** As detailed below, the Check Point R75 system satisfies all requirements of this claim element

735. As demonstrated above in relation to my analysis of claim element 1e, the packet transformation function performed by the packet security gateway includes not only blocking

and/or forwarding, but also recording functionality. More specifically, the log records shown in Figure 145 in the analysis of claim element 1f are records comprising a subset of the packet information.

736. Thus, for at least the same reasons as detailed above, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 1f.

737. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1f of the '213 Patent.

738. **Claim 1g: reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and** As detailed below, the Check Point R75 system satisfies all requirements of this claim element. I understand that the parties have agreed that the term "logging system standard" is to be construed as "a standard for logging information," and I have applied this construction throughout my analysis.

739. As demonstrated above in relation to my analysis for Claim 1, the Check Point R75 system logs packets "comprising application-layer packet-header information." Additionally, the Check Point R75 system can reformat the subset of information specified by the packet digest logging as shown in Figure 146. This reformatted graphical representation of the information is generated in the Check Point R75 SMS GUI by double-clicking on the packet as represented in the SmartView Tracker log in Figure 145.



Figure 146. Screenshot showing reformatted packet log information from Check Point R75.

740. Thus, for at least the same reasons as detailed above, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 1g.

741. Furthermore, the R75 documentation describes additional log export capabilities:[160] "While the SmartView Tracker is the standard log tracking solution, you may also wish to use your logs in other ways…. A log file can be exported in two different ways: as a simple text files; in a database format, exported to an external Oracle database. Smartview Tracker supports a basic export operation… you can create a comma delimited ASCII file that can be used as input for other applications." This documentation give examples of various standard formats that can be used for exporting log entries.

742. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1g of the '213 Patent.

743. **Claim 1h: routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.** As detailed below, the Check Point R75 system satisfies all requirements of this claim element.

744. As demonstrated above in relation to my analysis of Claim 1 the Check Point R75 system blocks or transmits traffic on a packet-by-packet basis. The Check Point R75 system can then be used to view the contents of the blocked packets, as these packets are routed to the Check Point log server, which performs the functionality of a monitoring device. For example, the screenshot shown in Figure 147 displays packet information routed from the packet security gateway to the log server.

[160] "Security Management Server R75 Administration Guide" (dated December 15, 2010) at page 74.



Figure 147. Screenshot of the Packet Capture View Output from Check Point R75

745. Thus, for at least the reasons detailed above, it is my opinion that the Check Point R75 system satisfies all requirements of claim element 1h.

746. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates claim element 1h of the '213 Patent.

747. Consequently, for at least the reasons above, it is my opinion that each and every element of Claim 1 of the '213 Patent is anticipated by the Check Point R75 system.

CENTRIPETAL-CSCO 087783

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 283

3. CLAIM 3

748. **The method of claim 1, wherein the at least one rule indicates performing a deny packet transformation function on the packets comprising the application-layer packet-header information, and wherein the performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information.** As detailed below, the Check Point R75 system satisfies all requirements of this claim.

749. As demonstrated above in relation to my analysis of Claim 1, a Check Point R75 policy rule corresponding to application-layer packet-header information was configured to block packets based on the specific HTTP application layer header content "SampleRequestHeader: 85." When an attempt was made to transmit packets with this specific header content from Computer B to Computer A, Check Point R75 performed "a deny packet transformation function," dropping the packet, and blocking it from being transmitted to Computer A. See, for example, Figure 139 and Figure 145.

750. Thus, for at least the reasons detailed above, it is my opinion that the Check Point R75 system satisfies all requirements of Claim 3.

751. Therefore, for at least the reasons given above, it is my opinion that the Check Point R75 system anticipates Claim 3 of the '213 Patent.

XIV. U.S. PATENT NO. 9,917,856

752. I have been asked to review the '856 Patent and assess the validity of Claims 1, 18, 24, and 25 therein in view of the prior art referenced below. I will first summarize the '856 patent briefly and then discuss claim-by-claim invalidity analysis.

A. SUMMARY OF THE '856 PATENT

753. The '856 patent assigned to Centripetal Networks, Inc., Herndon, VA (US), was filed on Dec. 23, 2015 and published on Mar. 13, 2018. The '856 patent relates to a rule-based network threat detection for encrypted communications. Specifically, it relates to a packet-filtering system that can distinguish between packets with unencrypted data versus encrypted data and then determine based on the unencrypted data corresponding to any network-threat indicators that encrypted data also corresponds to network threat indicators.[161]

754. Figure 148 illustrates an exemplar environment for rule-based network-threat detection for encrypted communications including "Network A" comprised of hosts, proxy devices (PDs), web proxy, rule gates (RGs), domain name system (DNS), internet content adaption protocol (ICAP) server and gateway (GW). Network B interfaces networks A with other networks, rule providers (RPs), threat-intelligence providers (TIPs), and other hosts.[162] Network-threat-intelligence providers communicate to rule providers regarding one or more network threats including one or more associated network threat indicators, e.g., network addresses, fully qualified domain names (FQDNs), and uniform resource identifiers (URIs). Based on this information, rule provider generates packet-filtering rules and communicates the rules to rule gates. [163]

[161] '856 patent, ay 1:24-45
[162] '856 patent, at 2:20-60.
[163] '856 patent, at 3:65-4:9.

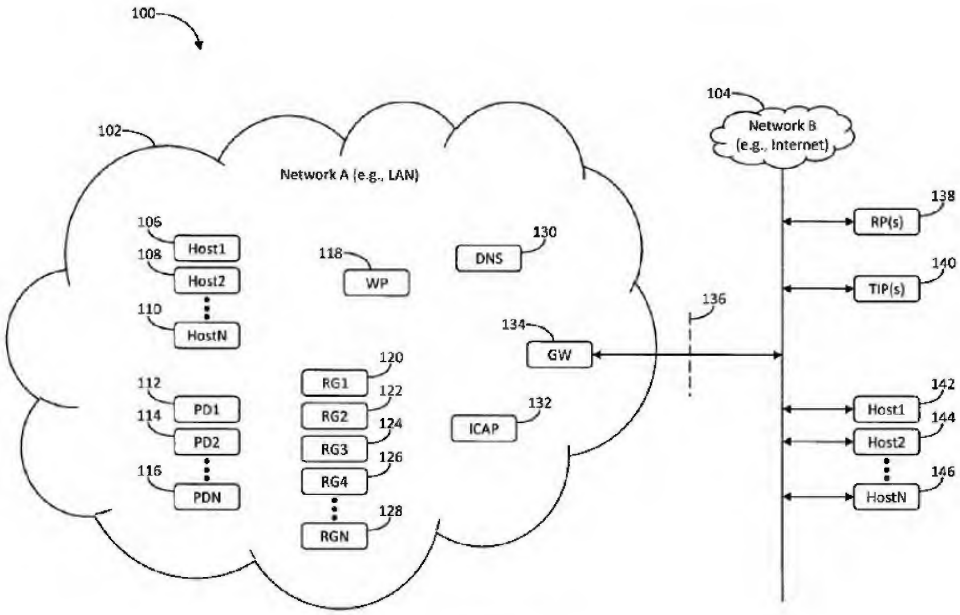


FIG. 1

Figure 148. An illustrative environment for rule-based network-threat detection for encrypted communications ('856 Patent, FIG.1).

755. Figure 149 illustrates a flow diagram for rule-based network-threat detection for encrypted communication. Packet filtering system receives packet filtering rules from rule providers. Based on packet-filtering rules, a packet filtering system will filter packets. Then packet filtering system will identify packets that have encrypted data and packets that have unencrypted data, e.g. packets comprising of DNS query, DNS reply, handshake message, etc. If the data in unencrypted packets correspond to network-threat indicators, then encrypted packets correlated to unencrypted packets are also assumed to correspond to network-threat indicators.[164] In some cases, such packets are dropped while in other case cases they may be routed via a proxy device.[165]

[164] '856 patent, at 23:63-24:30.
[165] '856 patent, at 5:10-14, 6:60-7:11

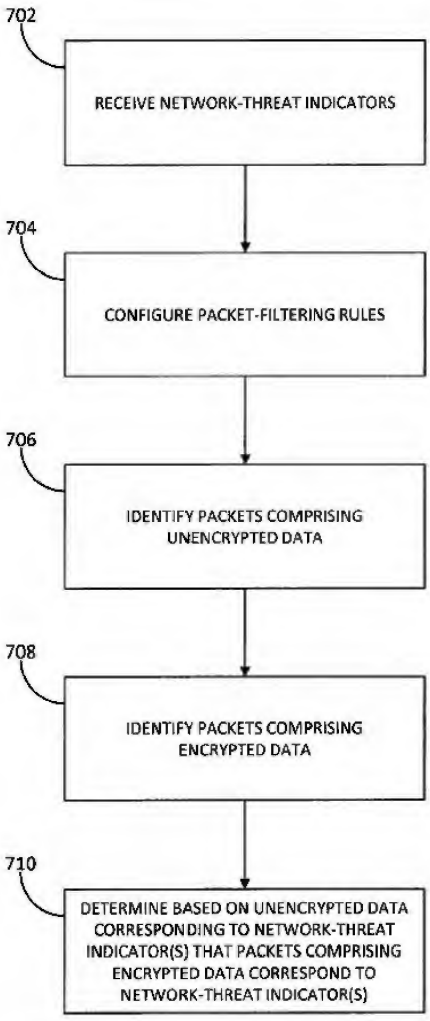


FIG. 7

Figure 149. An illustrative method for rule-based network-threat detection for encrypted communications ('856 Patent, FIG.7).

756. Packet-filtering system can correlate packets using network layer header information (e.g., protocol type, a destination network address, a source network address, a signature or authentication information), transport-layer information (e.g., a destination port, a source port, a checksum), application-layer information (e.g., a domain name, a uniform resource

locator (URL), a uniform resource identifier (URI)), other data in the packets, or environmental variables (e.g., time stamps).[166]

B. ANTICIPATION IN VIEW OF CHECK POINT R77

757. The Check Point R77 system was commercially available to purchase before the priority date of the '856 Patent. The Check Point R77 Security Gateway (SG)[167] performs the function of a packet-filtering device, and the Check Point R77 Security Management Server (SMS)[168] performs the function of a security policy management server, which is a centralized server for managing packet-filtering rules and packet-filtering devices

758. An illustration of how the R77 SG and R77 SMS fit into a typical network architecture is shown in Figure 150.



Item	Description
1	Internet and external networks
2	Security Gateway
3	SmartDashboard
4	Security Management Server
5	Internal network

Figure 150. Typical deployment of a security gateway and a security management server (configurable using the SmartDashboard graphical user interface, or GUI).[169]

759. I understand the Plaintiffs, in their infringement contentions, have accused Vision ONE of infringing the '856 Patent, even though this product does not include a separate proxy device. Based on this reading of the '856 Patent, with which I do not agree, Check Point R77 anticipates Claims 1, 18, 24, and 25 of the '856 Patent, as detailed below. In addition to the

[166] '856, at 5:31-6:6.
[167] See "Check Point R77 Firewall Administration Guide" (dated Aug 27, 2013).
[168] See "Check Point R77 Security Management Server Administration Guide" (dated Aug 27, 2013).
[169] See pp. 9–10 CP_R77_Firewall_AdminGuide.

analysis presented herein, further discussion of relevant testing is described in Appendix G, which I incorporate by reference.

1. TEST CONFIGURATION WITH CHECK POINT R77

760. Exponent procured the Check Point R77 SMS product and installed it on a 32-bit PC-compatible Dell Latitude E6400 computer using the "Check_Point_R77.20_T124_Install.Gaia.iso" DVD ISO image.[170] Exponent also procured the Check Point R77 SG product and installed it on two 32-bit PC-compatible Dell PowerEdge 1750 computers using the "Check_Point_R77.20_T124_Install.Gaia.iso" DVD ISO image. The SMS and SGs were installed in a "Distributed Deployment" configuration wherein the SMS is installed on a different machine than the SGs.

761. To demonstrate the functionality of the system, Exponent set up a test network to send traffic across the security gateway. Figure 151 shows the physical layout of the hardware used for Exponent's analysis, including the one security gateway (gw2), the security management server, the SmartDashboard (GUI), two switches, and two computers for sending and receiving packet traffic. Figure 152 shows the schematic layout of the test network used for Exponent's analysis. Network A includes Computer A, and Network B includes the Check Point R77 SMS along with Computer B. Security Gateway 1, which includes a packet-filtering device, protects Network B from Network A.

[170] According to the Check Point website, DVD installation material was available in December 2010 (see https://supportcenter.Check Point.com/supportcenter/) and the installation procedure for the Firewall and Security Management Server is documented in the "R75 Installation and Upgrade Guide."

CENTRIPETAL-CSCO 087789

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 289

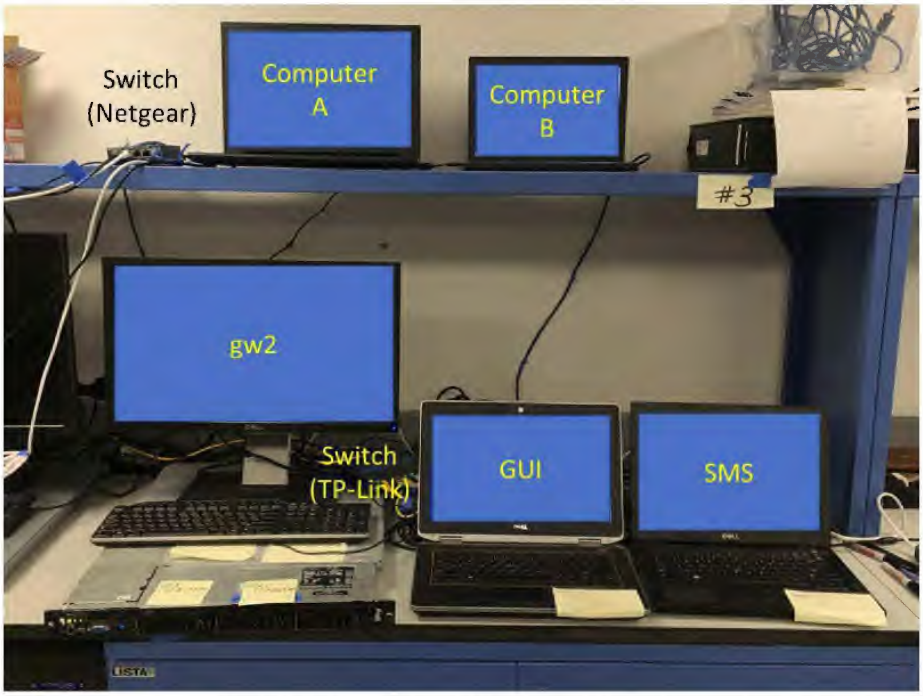


Figure 151. Image of test network hardware setup.

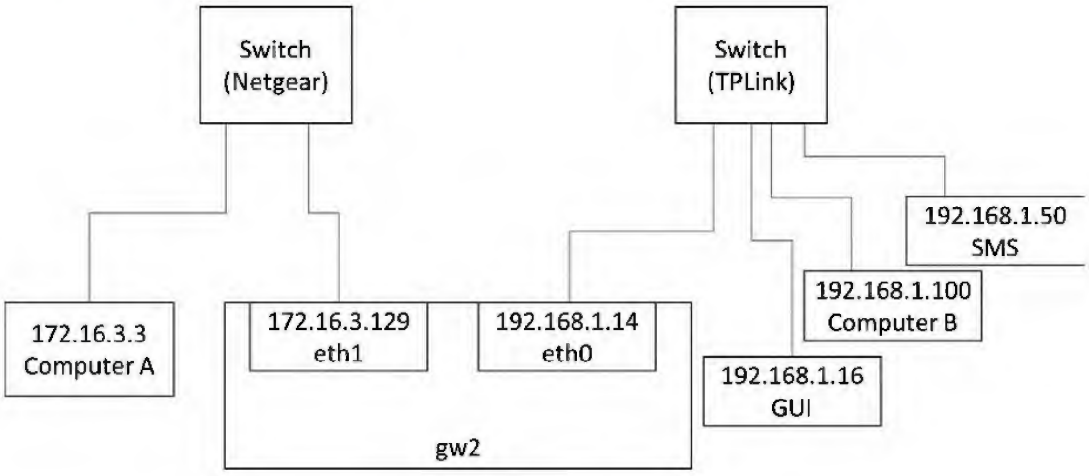


Figure 152. Network diagram of test setup

2. CLAIM 1

762. **Claim 1a: A method comprising: receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance**

with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat; As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

763. The Check Point R77 system is a network threat protection solution that includes the Check Point R77 Security Management Server (SMS) and one or more Check Point R77 Security Gateways (SGs). According to the Check Point R77 documentation,[171] the Security Management Server is "[t]he application that manages, stores, and distributes the Security Policy to the Security Gateways." A Security Gateway is "[a] computer or appliance that inspects traffic and enforces Security Policies for connected network resources," and the Security Policy is "[a] collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources through the use of packet inspection."(emphasis added). The method by which the Check Point R77 system provides network security involves filtering packets by applying a set of user-defined filters, including an option wherein said filter can comprise a domain name that is identified as a network threat, and in doing so satisfies all requirements of claim element 1a of the '856 Patent.

764. The '856 Patent specification makes many references to a "packet-filtering system," but provides no explicit definition of this term. It is my understanding that no claim construction has been submitted for the term "packet filtering system," with respect to the '856 Patent, and thus the plain and ordinary meaning should be applied. However, it is also my understanding that there was a dispute regarding the construction of a similar term in the Joint Claim Construction Statement[172] with respect to the '722 Patent. While I have applied

[171] See, generally, "CP_R77_SecurityManagement_AdminGuide.pdf" (dated 27 August 2013).
[172] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))

CENTRIPETAL-CSCO 087791

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 291

the plain and ordinary meaning to the term "packet filtering system" for the '856 Patent, because the '722 and '856 Patents have similar specifications, with similar or identical terms in the claim language, and address similar subject matters at similar points in time as would be understood by a similar POSITA, I have also considered the respective claim constructions addressed in the Joint Claim Construction Statement while performing my analysis herein.

765. I understand that in relation to the '722 Patent there is a dispute regarding the construction of the term "packet-filtering device." More specifically, Plaintiffs have proposed that this term be construed as "a device programmed to filter packets based on data associated with a packet," while Defendants have proposed that no construction is needed and that this term should be given its "plain meaning." I have considered both proposed constructions of the term "packet-filtering system," per the similar term in the Joint Claim Construction Statement, as well as the plain an ordinary meaning of this term as would have been understood by a POSITA at the time of the invention, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system comprises a "packet-filtering system," as explained below.

766. Similarly, the '856 Patent specification makes many references to "packet-filtering rules," but again provides no explicit definition of this term. I understand that in relation to the '856 Patent there is a dispute regarding the construction of the term "packet-filtering rules." More specifically, Plaintiffs have proposed that this term be construed as "condition or set of conditions that when satisfied cause a computing device to filter packets based on data associated with a packet," while Defendants have proposed "(i) packet-identifying

CENTRIPETAL-CSCO 087792

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 292

criteria and (ii) an operator to be performed on the identified packets." I have considered both proposed constructions of this term in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 receives "a plurality of packet-filtering rules," as detailed below.

767. The Check Point R77 system is intended to be located at the interface between two different machines or networks, such that packets sent between said machines or networks must pass through the Check Point R77 Security Gateway. For example, in the test configuration described above, the Check Point R77 SG 1 is located between Computers A and B such that packets are not sent directly between these machines, but rather are first received by SG 1, which then in turn can pass the communication to its intended destination. The Check Point R77 system does not have to forward all packets, however, and can instead perform a variety other functions, such as dropping, logging, rerouting, to packets that match certain criteria.

768. The Check Point R77 documentation states that "SmartDashboard may be installed on the Security Management server or on any other machine." SmartDashboard is the "set of GUI applications used to manage different aspects of the corporate network" referred to as "SmartConsole," which is "used to create, edit and install policies," and allows for the management of objects that "represent actual network components such as gateways, servers and networks."[173] In this respect, the criteria for identifying packets, and the functions that are performed on said packets, are determined using a set of filters that are configured by a user via the from the SmartDashboard GUI, associated with the Check Point R77 SMS, and communicated to the Check Point R77 SG(s). Each filter comprises at least one rule, which

[173] See p.10-11"Check Point R77 Security Management Server Administration Guide" (dated Aug 27, 2013).

CENTRIPETAL-CSCO 087793

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 293

specifies at least one criteria used to determine which packets are subject to the at least one rule, and at least one function that is to be performed on such packets.

769. Thus, at least because the Check Point R77 SG is programmed with rules, communicated by the Check Point R77 SMS, that filter packets according to criteria that may be based on data associated with the packet (such as IP addresses, URLs, packet data content, etc.) the Check Point R77 SG constitutes a "device programmed to filter packets based on data associated with a packet," which satisfies Plaintiff's proposed construction for "packet-filtering device."

770. Also, in my opinion, a POSITA would recognize that the "plain meaning" for "packet-filtering device" is also satisfied by the Check Point R77 SG, at least because the Check Point R77 SG is a device that filters packets, and thus Defendants' proposed construction for "packet-filtering device" is also satisfied. Also, I note that each filter causes the Check Point R77 SG to filter packets based on data associated with each packet, at least because the Check Point R77 SG applies filters only to packets that match the applicable condition or conditions of the criteria of said filter: thus the filters satisfy Plaintiff's proposed construction for "packet-filtering rules." Similarly, at least because each filter comprises a criteria, which constitutes "packet-identifying criteria" and a function to be performed on matching packets, which constitutes "an operator to be performed on the identified packets," the filters satisfy Defendants' proposed construction for "packet-filtering rules."

771. Moreover, at least because the laptop running the security gateway and the laptop running the security management server (SMS) with its associated SmartDashboard graphical user interface (GUI) are comprised of components that include both "a hardware processor" and "a memory," the Check Point R77 system also satisfies the claim requirement of a packet-

filtering system that is comprised of "a hardware processor and a memory," configured to filter packets in accordance with a plurality of packet filtering rules.

772. As with the terms "packet-filtering system" and "packet-filtering rules," the '856 Patent specification makes many references to "network-threat indicators," as a means of filtering transmitted packet information, but does not define what constitutes a "network-threat indicator. I understand that the parties have agreed that the term "network-threat indicators" is to be construed as "indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like." I have applied this construction throughout my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. In any event, the Check Point R77 system comprises a method which includes "network-threat indicators" indicated by data received from the packet filtering system, in accord with the associated packet filtering rules, as required by this claim element.

773. Exponent has demonstrated on the Check Point R77 system test setup that user-defined packet-filtering rules can be sent to one or more packet-filtering devices, and then configured and deployed by creating "security policies" and installing those policies on selected security gateways.[174] The policies that are installed on the gateway may correspond to specific network threats.[175] Amongst the plurality of packet-filtering rules that can be installed on the Check Point R77 system, Exponent has shown that the system enables the ability to install packet-filtering rules for blocking packets associated with specific domain names when said domain names are designated to constitute a "network threat" within the packet-filtering rule

[174] See, generally, "CP_R77_SecurityManagement_AdminGuide.pdf" (dated 27 August 2013) and "CP_R77_Firewall_AdminGuide.pdf" (dated 27 August 2013).

[175] See "CP_R77_Firewall_AdminGuide.pdf" (dated 27 August 2013) at Chapters 7 and 8.

configurations. To demonstrate this, a domain-specific blocking rule was defined for a domain named "patent856.com", as shown in Figure 153.

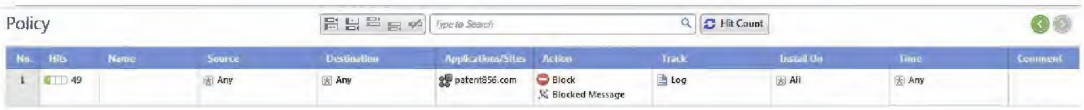


Figure 153. Rule blocking the "patent856.com" domain

774. In Exponent's Check Point R77 system test setup, SG 1 serves as a packet-filtering device and can be configured to identify packets based on numerous other packet-filtering rules pertaining to numerous other network threat indicators that are also installed by default on the Check Point R77 system, as shown in Figure 154. This figure further shows that the Check Point R77 SG is not limited to receiving a single packet filtering rule, but can in fact receive a plurality of such rules corresponding to various network threats.

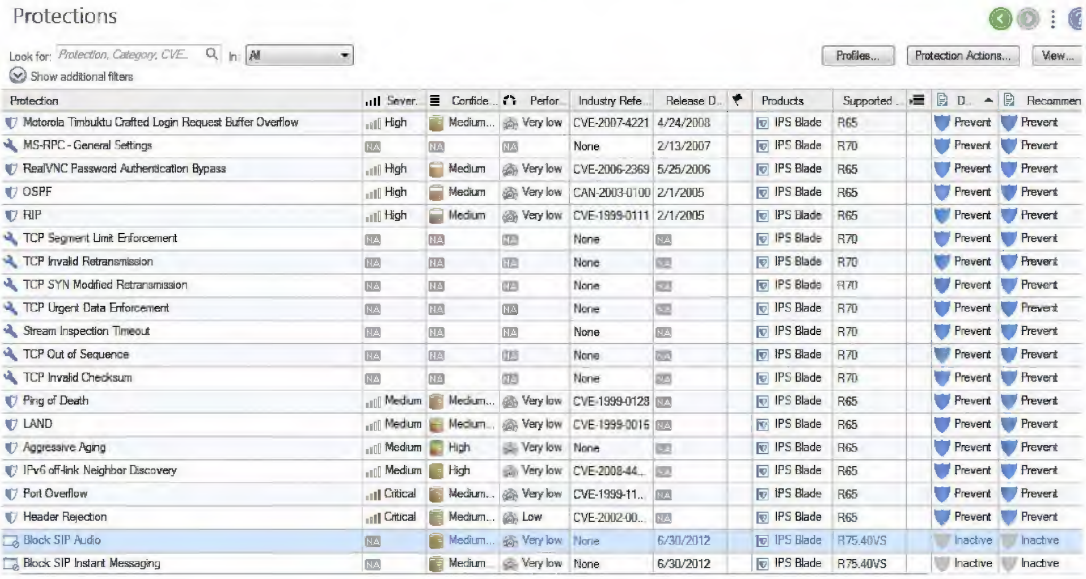


Figure 154. Examples of IPS protections, including those which are enforced for the current test setup.

775. A final rule was also set for the firewall to accept packets that are not blocked by any of the other rules of the system (Figure 155).

CENTRIPETAL-CSCO 087796

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 296



Figure 155. Screenshot showing a final allow rule, which applies to any traffic that is not blocked by the other rules.

776. In the test setup used to demonstrate that the Check Point R77 system satisfies all limitations of Claim 1 of the '856 Patent, Exponent used Computer A (IP 172.16.3.3) to host an HTTP server, using the python SimpleHTTPServer module. The "hosts" file on computer B was then used to route traffic for a given domain to a specific IP address. In the example in Figure 156, the "Patent856.com" domain name is associated with the IP address of Computer A.

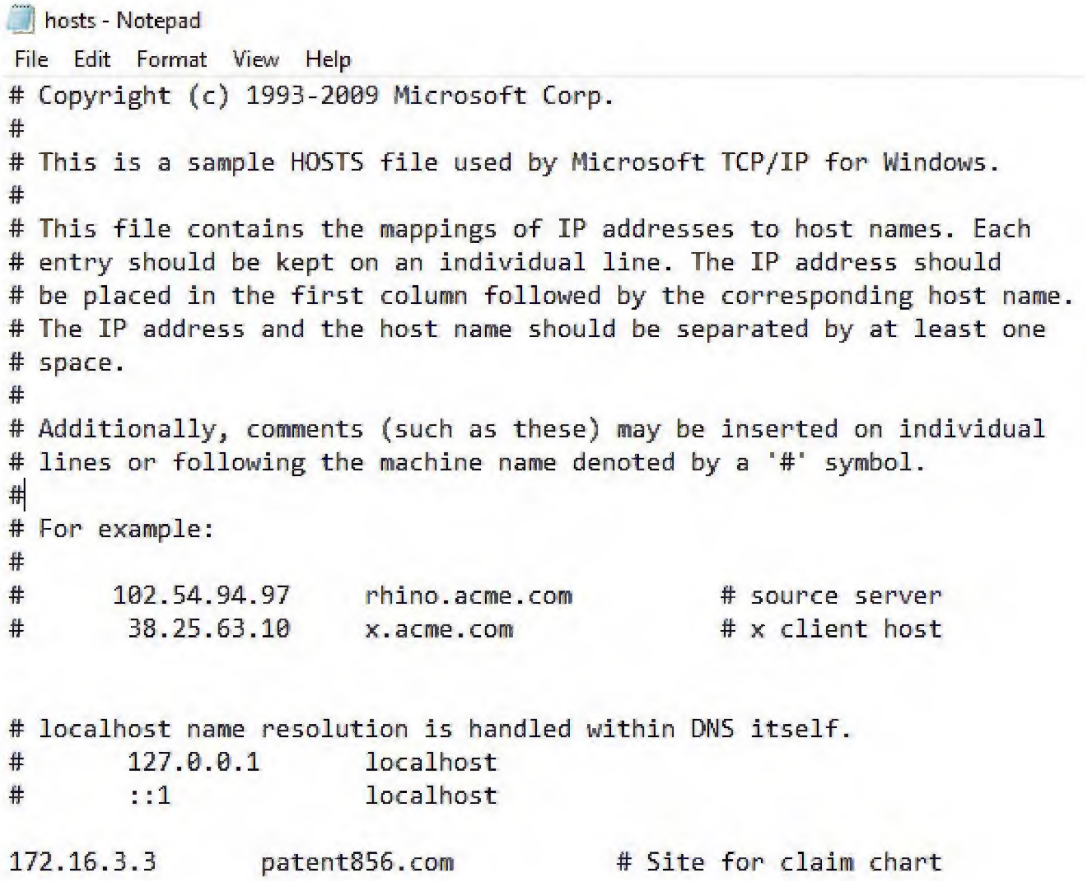


Figure 156. Hosts file relating the domain name "patent856.com" to the IP address 172.16.3.3

777. The server was hosted on port 8000 of Computer A, as shown in Figure 157 below.



Figure 157. Hosting on Port 8000 of Computer A

778. The hosts file in Computer B was then modified to direct traffic from "patent857.com" to IP address 172.16.3.3, as shown in Figure 158. When "http://patent857.com:8000" is typed into a web browser on Computer B, the webpage hosted on Computer A is accessed successfully (Figure 159).

```
172.16.3.3        patent857.com              # Site for claim chart
```

Figure 158. Initial test set up for the hosts file to associate the domain name "patent857.com" with IP address 172.16.3.3

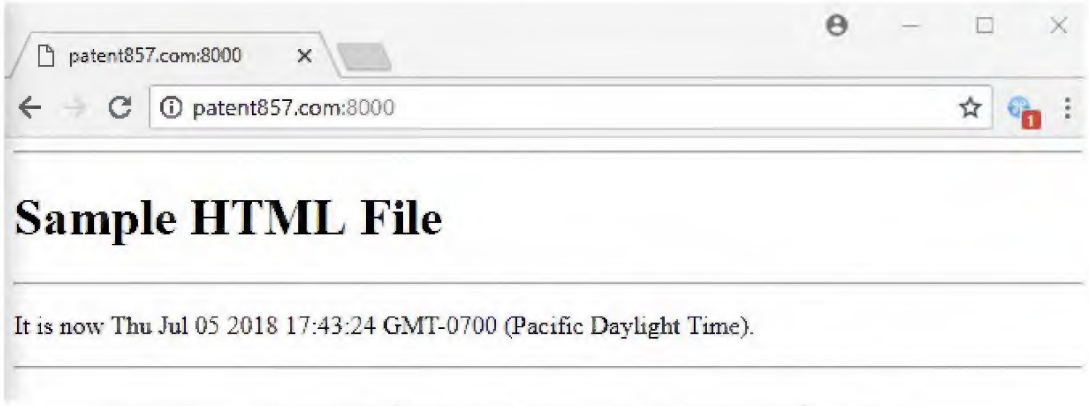


Figure 159. Display from Computer B of the HTML file hosted on Computer A

779. Next, the hosts file was modified to route requests for "patent856.com" to IP address 172.16.3.3 (Figure 160).

```
172.16.3.3        patent856.com              # Site for claim chart
```

Figure 160. Modification to the hosts file to associate the domain name "patent856.com" with the IP address 172.16.3.3.

780. In this case, because the domain name is "patent856.com" rather than "patent857.com" access to the HTML page is blocked by the gateway (Figure 161). As shown in Figure 161, because the access was blocked, the request is re-routed and a default page from a different machine is displayed rather than the HTML page hosted on Computer A.

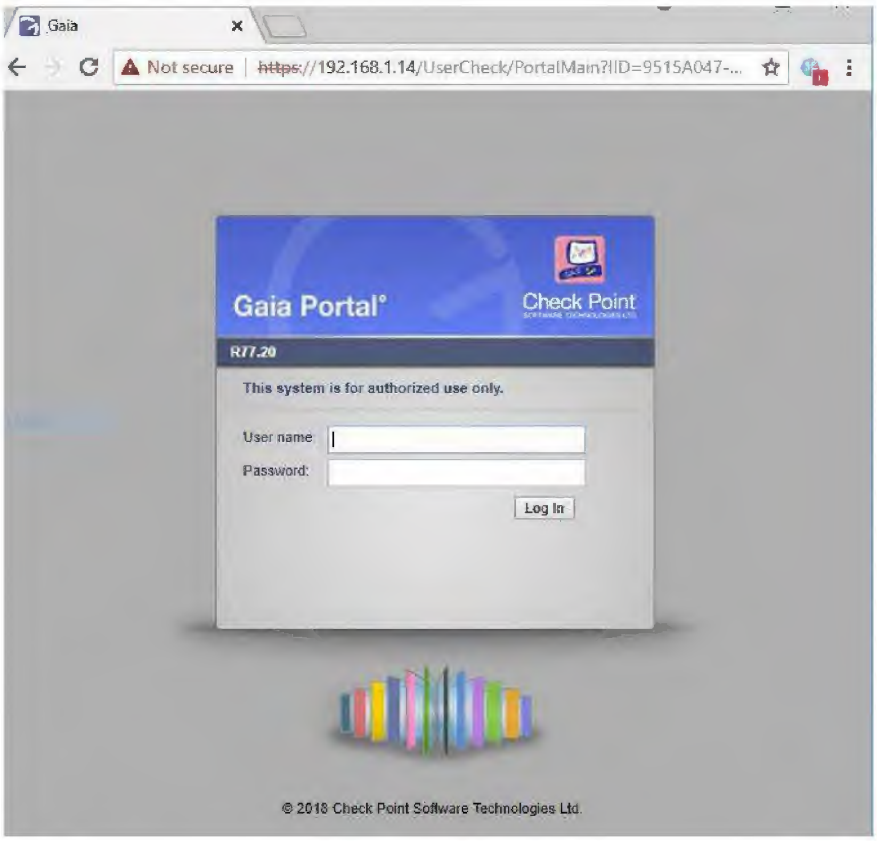


Figure 161. Screenshot from Computer A indicating that access to the "patent856.com" domain was blocked by the gateway.

781. Hence, Exponent has demonstrated that the Check Point R77 system includes a packet-filtering system which filters packets in accordance with a plurality of packet-filtering rules, and operates a method in which said packet-filtering rules receive data indicating a plurality of network-threat indicators wherein at least one of the network-threat indicators comprises a domain name identified as a network threat. Thus, for at least the reasons detailed above, Exponent has demonstrated that the Check Point R77 system operates a method that satisfies the requirements of this claim element 1a of the '856 Patent.

782. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 1a of the '856 Patent.

783. **Claim 1b: identifying packets comprising unencrypted data;** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

784. The Check Point R77 system operates a method that satisfies the requirements of claim element 1a, as described above, and furthermore includes identifying packets comprising unencrypted data. This can be most effectively illustrated by demonstrating the manner in which the transmission of both encrypted and unencrypted data packets can be selectively blocked or allowed by a packet filtering device in the Check Point R77 system.

785. For example, using the test setup described above, Exponent has demonstrated that the Check Point R77 system enables the ability to block encrypted HTTPS traffic, which can be accomplished by de-selecting "Categorize HTTPS sites" in the firewall options menu of the SMS GUI (Figure 162).



Figure 162. HTTPS sites are not categorized.

786. Using the python modules "SimpleHTTPServer," "BaseHTTPServer," and "ssl," an HTTPS site was hosted on Computer A (Figure 163), which was successfully accessed by Computer B at the patent856.com domain (Figure 164).

```
exponent@adam-jumpkit:~/Desktop/https_server$ python -m https_server
Enter PEM pass phrase:
```

Figure 163. HTTPS server hosted on computer A

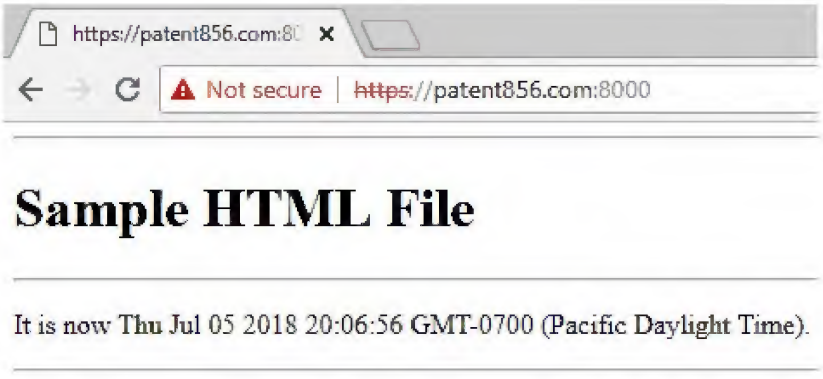


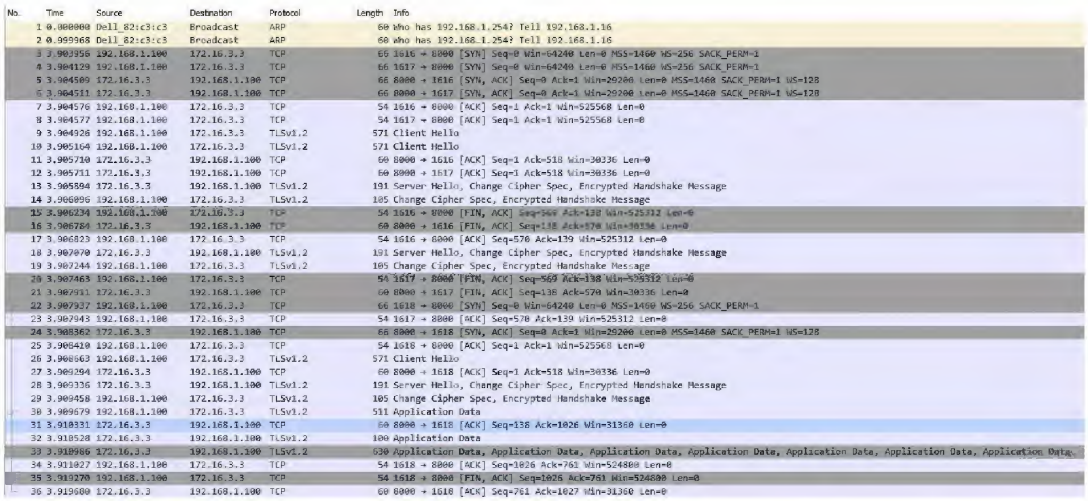
Figure 164. Successful loading of HTTPS site

787. The Python server on Computer A shows a successful access by Computer B (Figure 165):

```
exponent@adam-jumpkit:~/Desktop/https_server$ python -m https_server
Enter PEM pass phrase:
192.168.1.100 - - [05/Jul/2018 20:05:16] "GET / HTTP/1.1" 200 -
```

Figure 165. Computer B successfully accessed HTTPS site hosted son Computer A.

788. Wireshark (Figure 166) was then used to show the successful communication of unencrypted packets (during and prior to completion of the TLS handshake) as well as the encrypted packets (transmitted after completion of the TLS handshake).



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_82:c3:c3	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.16
2	0.999968	Dell_82:c3:c3	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.16
3	3.903956	192.168.1.100	172.16.3.3	TCP	66	1616 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	3.904129	192.168.1.100	172.16.3.3	TCP	66	1617 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	3.904509	172.16.3.3	192.168.1.100	TCP	66	8000 → 1616 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
6	3.904511	172.16.3.3	192.168.1.100	TCP	66	8000 → 1617 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
7	3.904576	192.168.1.100	172.16.3.3	TCP	54	1616 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0
8	3.904577	192.168.1.100	172.16.3.3	TCP	54	1617 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0
9	3.904926	192.168.1.100	172.16.3.3	TLSv1.2	571	Client Hello
10	3.905164	192.168.1.100	172.16.3.3	TLSv1.2	571	Client Hello
11	3.905710	172.16.3.3	192.168.1.100	TCP	60	8000 → 1616 [ACK] Seq=1 Ack=518 Win=30336 Len=0
12	3.905711	172.16.3.3	192.168.1.100	TCP	60	8000 → 1617 [ACK] Seq=1 Ack=518 Win=30336 Len=0
13	3.905884	172.16.3.3	192.168.1.100	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
14	3.906096	192.168.1.100	172.16.3.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
15	3.906234	192.168.1.100	172.16.3.3	TCP	54	1616 → 8000 [FIN, ACK] Seq=569 Ack=138 Win=525312 Len=0
16	3.906784	172.16.3.3	192.168.1.100	TCP	60	8000 → 1616 [FIN, ACK] Seq=138 Ack=570 Win=30336 Len=0
17	3.906823	192.168.1.100	172.16.3.3	TCP	54	1616 → 8000 [ACK] Seq=570 Ack=139 Win=525312 Len=0
18	3.907070	172.16.3.3	192.168.1.100	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
19	3.907244	192.168.1.100	172.16.3.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
20	3.907463	192.168.1.100	172.16.3.3	TCP	54	1617 → 8000 [FIN, ACK] Seq=569 Ack=138 Win=525312 Len=0
21	3.907931	172.16.3.3	192.168.1.100	TCP	60	8000 → 1617 [FIN, ACK] Seq=138 Ack=570 Win=30336 Len=0
22	3.907937	192.168.1.100	172.16.3.3	TCP	66	1618 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	3.907943	192.168.1.100	172.16.3.3	TCP	54	1617 → 8000 [ACK] Seq=570 Ack=139 Win=525312 Len=0
24	3.908362	172.16.3.3	192.168.1.100	TCP	66	8000 → 1618 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
25	3.908410	192.168.1.100	172.16.3.3	TCP	54	1618 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0
26	3.908663	192.168.1.100	172.16.3.3	TLSv1.2	571	Client Hello
27	3.909294	172.16.3.3	192.168.1.100	TCP	60	8000 → 1618 [ACK] Seq=1 Ack=518 Win=30336 Len=0
28	3.909336	172.16.3.3	192.168.1.100	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
29	3.909458	192.168.1.100	172.16.3.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
30	3.909679	192.168.1.100	172.16.3.3	TLSv1.2	511	Application Data
31	3.910331	172.16.3.3	192.168.1.100	TCP	60	8000 → 1618 [ACK] Seq=138 Ack=1026 Win=31360 Len=0
32	3.910528	172.16.3.3	192.168.1.100	TLSv1.2	100	Application Data
33	3.910986	172.16.3.3	192.168.1.100	TLSv1.2	630	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data,
34	3.911027	192.168.1.100	172.16.3.3	TCP	54	1618 → 8000 [ACK] Seq=1026 Ack=761 Win=524800 Len=0
35	3.911270	192.168.1.100	172.16.3.3	TCP	54	1618 → 8000 [FIN, ACK] Seq=1026 Ack=761 Win=524800 Len=0
36	3.911600	172.16.3.3	192.168.1.100	TCP	60	8000 → 1618 [ACK] Seq=761 Ack=1027 Win=31360 Len=0

Figure 166. Screenshot from Wireshark packet capture session showing a successful TLS handshake and subsequent transmission of encrypted application data.

789. After showing the successful transmission of HTTPS packets, the "Categorize HTTPS sites" box was selected in the firewall options menu of the SMS GUI (Figure 167).



Figure 167. "Categorize HTTPS sites" blocks sites with the HTTPS domain name.

790. When an attempt was made to access the HTTPS server on Computer A using a browser on Computer B, the page was unable to load (See Figure 167 and Figure 168).

```
exponent@adam-jumpkit:~/Desktop/https_server$ python -m https_server
Enter PEM pass phrase:
```

Figure 168. HTTPS server hosting the same website. This figure shows the initial startup of the server, but no subsequent activity, which indicates that it did not receive any requests from Computer B.

CENTRIPETAL-CSCO 087803

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 303

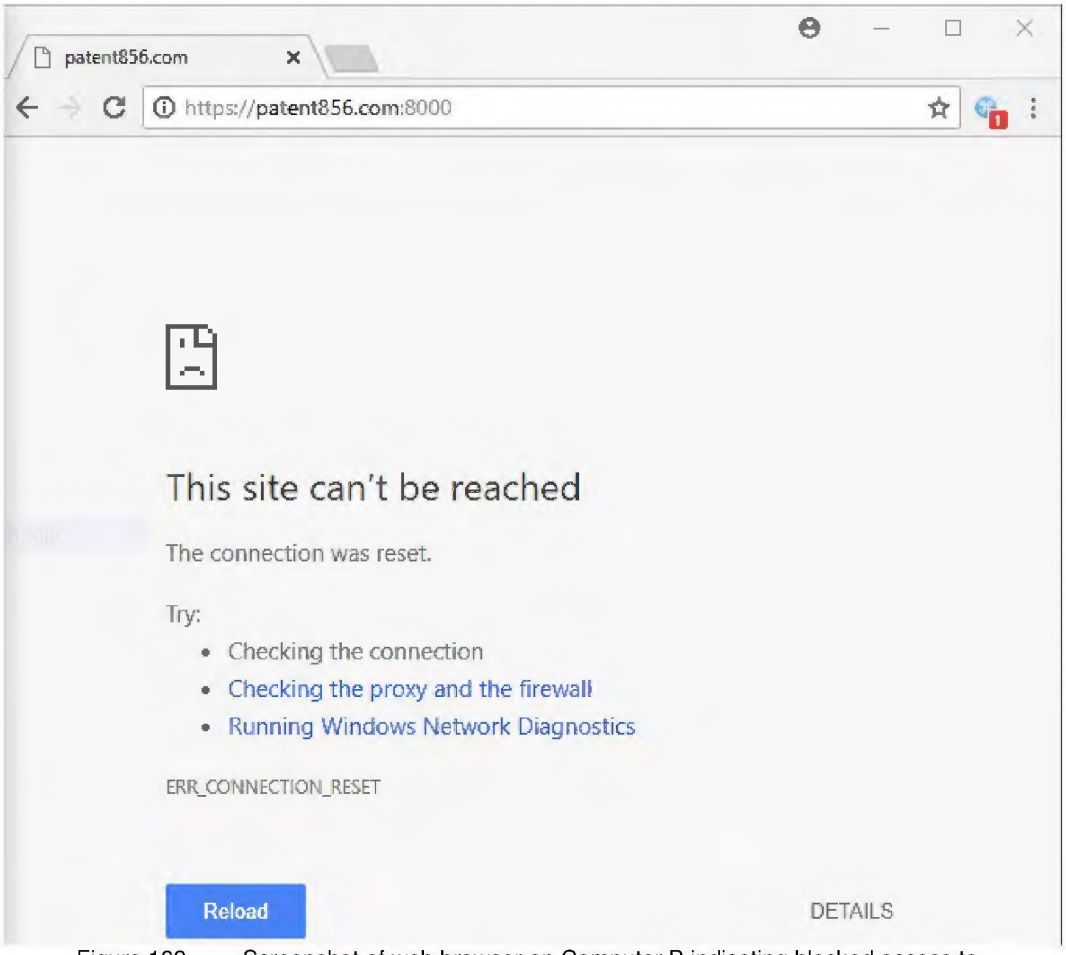


Figure 169. Screenshot of web browser on Computer B indicating blocked access to https://patent856.com:8000

791. Furthermore, the Wireshark information captured during the blocked attempt to access the HTTPS site shows that the TCP/IP handshake was completed, but the TLS handshake was not completed because packets were blocked. For example, the "Client Hello" was still transmitted, but the server did not respond with a "Server Hello" because the packets were blocked.

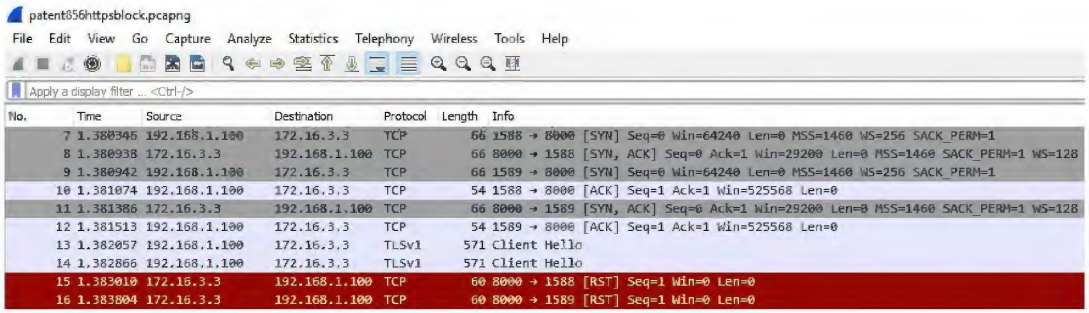


Figure 170. Screen Capture from Wireshark session running on Computer B showing that the HTTPS server does not respond with a "Server Hello."

792. Hence, as shown in the demonstration above, packets containing unencrypted data, such as the IP addresses in the packet headers, are identified and either blocked or allowed by the Check Point R77 system. Thus, for at least the reasons detailed above, the Check Point R77 system satisfies the requirements of claim element 1b of the '856 Patent.

793. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 1b of the '856 Patent.

794. **Claim 1c: identifying packets comprising encrypted data;** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

795. The above analysis for claim element 1b shows that packets comprising unencrypted data are identified, but it also clearly shows that packets containing *encrypted* data, such as the encrypted HTTP application data following the TLS handshake, are identified and either blocked or allowed by the Check Point R77 system.

796. In addition, according to the Check Point R77 documentation, encrypted packets can be identified and screened via "HTTPS Inspection" available on Check Point R77 system. For example, page 40 of the Check Point R77 Application Control and URL Filtering

Administration Guide indicates the use of HTTPS inspection via predefined rules, as shown in Figure 171.



Predefined Rule

When you enable HTTPS inspection, a predefined rule is added to the HTTPS Rule Base. This rule defines that all HTTPS and HTTPS proxy traffic from any source to the internet is inspected on all blades enabled in the Blade column. By default, there are no logs.

Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Certificate
Predefined Rule	Any	Internet	https HTTP_and_HTTPS_proxy	Any	Inspect	None	All	All	Outbound Certificate

Figure 171. Image from page 40 of Check Point R77 Application Control and URL Filtering Administration Guide

797. Page 41of the Check Point R77 Application Control and URL Filtering Administration Guide provides further information about the manner in which the "action" acts upon the filtered traffic, stating

> **Action**
> The action is what is done to the traffic. Click in the column to see the options and select one to add to the rule.
> - **Inspect** - The traffic is inspected on the blades set in the Blades column.
> - **Bypass** - The traffic of source and destination traffic in rules that include the bypass action are not decrypted and inspected. You can bypass HTTPS inspection for all Check Point objects. This is recommended for Anti-Bot, Anti-Virus, URL Filtering, and IPS updates. Other HTTPS protections that already operate on traffic will continue to work even when the HTTPS traffic is not decrypted for inspection.

798. See also, page 35 of the Check Point R77 Application Control and URL Filtering Administration Guide, which states "[y]ou can enable HTTPS traffic inspection on Security Gateways to inspect traffic that is encrypted by the Secure Sockets Layer (SSL) protocol."

799. Page 35 of the Check Point R77 Application Control and URL Filtering Administration Guide also indicates the two types of HTTPS inspection that may be applied:

There are two types of HTTPS inspection:

- **Inbound HTTPS inspection** - To protect internal servers from malicious requests originating from the internet or an external network
- **Outbound HTTPS inspection** - To protect an organization from malicious traffic being sent by an internal client to a destination outside of the organization.

800. This same page of the manual provides further description of the HTTPS inspection process, stating

> ## How it operates
>
> In outbound HTTPS inspection, when a client in the organization initiates an HTTPS connection to a secure site, the Security Gateway:
>
> 1. Intercepts the request.
> 2. d Establishes a secure connection to the requested web site and validates the site server certificate.
> 3. Creates a new SSL certificate for the communication between the Security Gateway and the client, sends the client the new certificate and continues the SSL negotiation with it.
> 4. Using the two SSL connections:
>   a. It decrypts the encrypted data from the client.
>   b. Inspects the clear text content for all blades set in the Policy.
>   c. Encrypts the data again to keep client privacy as the data travels to the destination web server resource.
>
> In inbound HTTPS inspection, when a client outside of the organization initiates an HTTPS connection to a server behind the organization's gateway, the Security Gateway:
>
> 1. Intercepts the request.
> 2. Uses the server's original certificate and private key to initiate an SSL connection with the client.
> 3. Creates and establishes a new SSL connection with the web server.
> 4. Using the two SSL connections:
>   a. It decrypts the encrypted data from the client.
>   b. Inspects the clear text content for all blades set in the policy.

c. Encrypts the data again to keep client privacy as the data travels to the destination server behind the gateway.

801. Lastly, page 36 of the Check Point R77 Application Control and URL Filtering Administration Guide provides the following instruction regarding how to enable HTTPS inspection on the Check Point R77 security gateways, stating "You must enable HTTPS inspection on each Security Gateway. From **Security Gateway > HTTPS Inspection > Step 3 >** Select **Enable HTTPS Inspection."**

802. Thus, for at least the reasons detailed above, the Check Point R77 system operates a method that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 1c of the '856 Patent.

803. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 1c of the '856 Patent.

804. **Claim 1d: determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

805. As demonstrated above, in relation to claim element 1a, the Check Point R77 system is capable of performing domain-specific blocking for HTTP files. Although some of the packets involved in HTTPS communication contain encrypted data, the domain name can be transmitted as unencrypted data, as is shown in the handshake data packet in Figure 172.

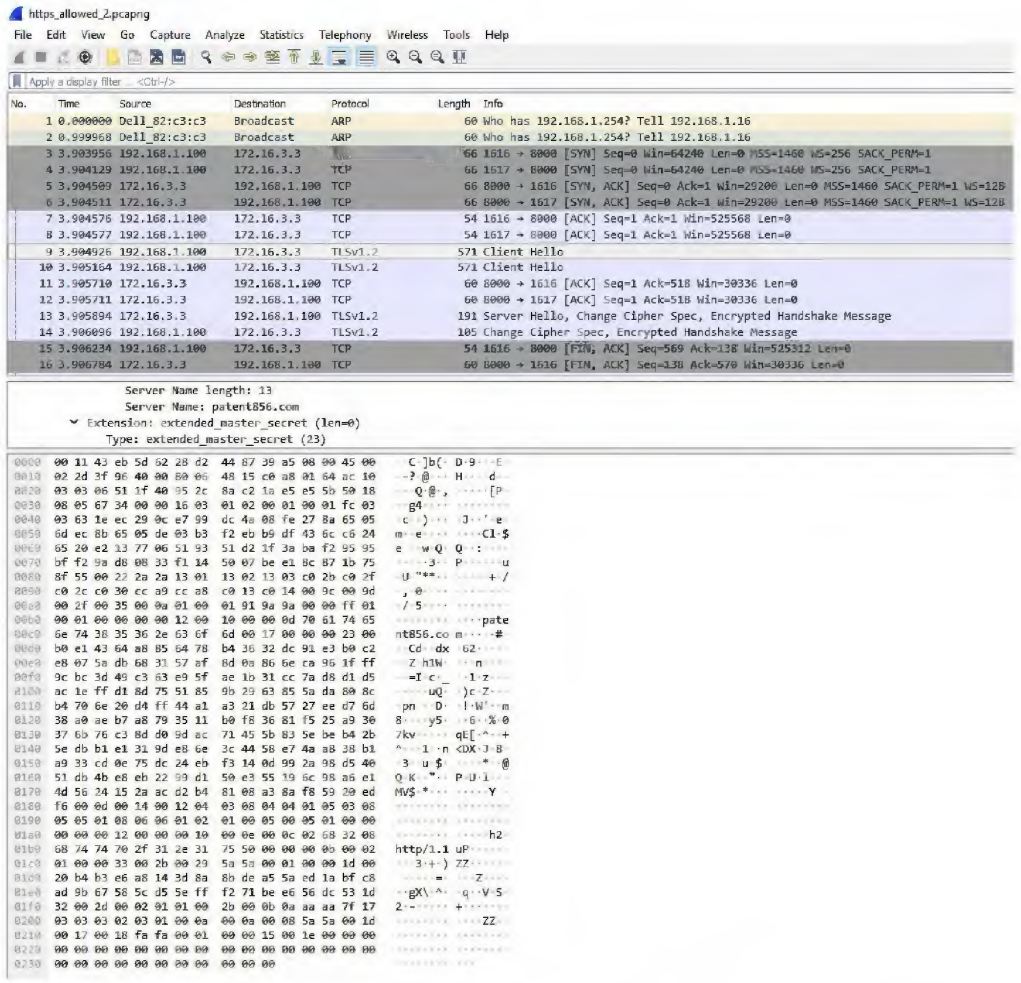


Figure 172. "Client Hello" packet during https handshake, showing "Patent856.com" as an unencrypted segment in the packet (lines 00c0 and 00d0).

806. Furthermore, additional information such as the IP packet header information is also unencrypted data. Therefore, the method employed by the Check Point R77 system of determining "packets comprising encrypted data that corresponds to the one or more network-threat indicators" is based on unencrypted data. Thus, for at least the reasons detailed above, the Check Point R77 system operates a method that satisfies the requirements of claim element 1d of the '856 Patent.

807. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 1d of the '856 Patent.

808. **Claim 1e: filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

809. As demonstrated above, in relation to claim element 1a, the Check Point R77 system is capable of performing URI-specific blocking, in which setting a block for http://patent856.com prevented access to the site, but access to http://patent857.com was permitted. Thus, Exponent has shown that the Check Point R77 system operates a method wherein the packet-filtering system filters packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators] based on a URI specified by a packet-filtering rule.

810. In addition to the testing performed by Exponent, the documentation for the Check Point R77 system also indicates that its packet filtering system can filter packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators based on data indicating a protocol version specified by the plurality of packet-filtering rules,

data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules. For example, page 39 of the Check Point R77 Application Control and URL Filtering Administration Guide describes how the HTTPS Inspection Policy performs traffic inspection, stating

> The HTTPS inspection policy determines which traffic is inspected. The primary component of the policy is the Rule Base. The rules use the categories defined in the Application and URL Filtering Database, network objects and custom objects (if defined).

811. Furthermore, page 40 of the Check Point R77 Application Control and URL Filtering Administration Guide outlines how predefined rules can be used to inspect and filter, as shown in Figure 173.



Figure 173. Image from page 40 of Check Point R77 Application Control and URL Filtering Administration Guide

812. Further description of how HTTPS packets are inspected is provided on page 40 of the Check Point R77 Application Control and URL Filtering Administration Guide, stating

> By default, HTTPS traffic on port 443 and HTTP and HTTPS proxy on port 8080 is inspected. You can include more services and ports in the inspection by adding them to the services list. To select other HTTPS/HTTP services, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of services and select a service. Other services, such as SSH are not supported.

813. Thus, for at least the reasons detailed above, the Check Point R77 system operates a method that satisfies the requirements of claim element 1e of the '856 Patent.

814. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 1e of the '856 Patent.

815. **Claim 1f: the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

816. As demonstrated above, in relation to claim element 1a, the packets related to domain "patent856.com" were filtered by the Check Point R77 system.

817. In addition to the testing performed by Exponent, the documentation for the Check Point R77 system also indicates that its packet filtering system can filter the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators based on data parameters listed in claim element 1e. For example, page 35 of the Check Point R77 Application Control and URL Filtering Administration Guide describes the process of HTTPS inspection, stating

> **How it operates**
> In outbound HTTPS inspection, when a client in the organization initiates an HTTPS connection to a secure site, the Security Gateway:
> 5. Intercepts the request.
> 6. d Establishes a secure connection to the requested web site and validates the site server certificate.
> 7. Creates a new SSL certificate for the communication between the Security Gateway and the client, sends the client the new certificate and continues the SSL negotiation with it.
> 8. Using the two SSL connections:
>   a. It decrypts the encrypted data from the client.
>   b. Inspects the clear text content for all blades set in the Policy.

c. Encrypts the data again to keep client privacy as the data travels to the destination web server resource.

In inbound HTTPS inspection, when a client outside of the organization initiates an HTTPS connection to a server behind the organization's gateway, the Security Gateway:

5. Intercepts the request.
6. Uses the server's original certificate and private key to initiate an SSL connection with the client.
7. Creates and establishes a new SSL connection with the web server.
8. Using the two SSL connections:
    a. It decrypts the encrypted data from the client.
    b. Inspects the clear text content for all blades set in the policy.
    c. Encrypts the data again to keep client privacy as the data travels to the destination server behind the gateway.

818. Hence, the Check Point R77 documentation includes descriptions of how the policy defined by the Check Point R77 system can be used to determine how encrypted packets are filtered. Thus, for at least the reasons detailed above, the Check Point R77 system operates a method that satisfies the requirements of claim element 1f of the '856 Patent.

819. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 1f of the '856 Patent.

820. **Claim 1g: routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

821. I understand there is a dispute regarding the construction of the term "proxy system," in relation to the '856 Patent. More specifically, in the Joint Claim Construction Statement[176] Plaintiff has proposed that this term be given its plain and ordinary meaning, while Defendants have proposed that this term be construed as a "system that establishes connections to devices in trusted and untrusted environments and relays packets between a device in the trusted environment and a device in the untrusted environment".[177] I have considered both proposed constructions in my analysis in addition to the description of this term within the '856 Patent specification, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Check Point R77 system satisfies all requirements of this claim element, for at least the reasons detailed below.

822. The documentation for the Check Point R77 system indicates that its packet filtering system can route "filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators," and in doing so satisfies the required functionality of this claim element.

823. For example, page 55 of Check Point IPS Administration Guide R77 ("Working with Packet Information") describes how packet capture is possible, stating

> **Capturing a Packet for Every Log**
> To capture packet data for a protection for every malicious packet that is logged, turn on the packet capture option in that protection. This attaches a packet capture to every log generated by the protection.
>
> In the middle manual also said that it can log every packet, but default is just log the first packet. We have the option to switch it.

[176] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))
[177] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

824. Although the manual also states that every packet can be logged, the default is to log the first packet only. Page 56 of the Check Point IPS Administration Guide R77 goes on to indicate how this can be switched, stating

> **Viewing Packet Capture Data in SmartView Tracker**
> A packet capture is automatically attached to the first packet logged by a protection since policy installation. If packet capture is turned on for a protection, a packet capture is attached to every log generated by the protection.
>
> **To view packet captures in SmartView Tracker**
> From the protection page that has Capture Packets selected, click View Logs
>
> > SmartView Tracker opens. Wait until the log window for the specific protection opens. Note - SmartView Tracker displays the current log file. If you have performed a log switch and the capture is in a different file, open that log file instead

825. Hence, for at least the reasons detailed above, the Check Point R77 system operates a method that satisfies the requirements of claim element 1g of the '856 Patent, and thus it is my opinion that the Check Point R77 system anticipates claim element 1g of the '856 Patent.

826. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates each and every element of Claim 1 of the '856 Patent.

3. CLAIM 18

827. **Claim 18a: The method of claim 1, wherein the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:** This claim is dependent upon Claim 1 of the '856 Patent, and as detailed above it is my opinion that Claim 1 is anticipated by the Check Point

R77 system. As detailed below, the Check Point R77 system also satisfies all limitations added to Claim 1 of the '856 Patent by Claim 18 therein.

828. I understand that the parties have agreed that the term "handshake messages" is to be construed as "messages to establish a session or connection,"[178] and I have applied this construction throughout my analysis herein.

829. The HTTPS communications observed during the testing detailed in relation to claim elements 1a and 1b include a TLS handshake to setup the encrypted channel. The Wireshark screenshot in Figure 166 shows the handshake and subsequent transfer of data from the client to the server.

830. Hence, the Check Point R77 system performs the method of Claim 1 wherein the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, as required by claim element 18a.

831. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirement of Claim 1 of the '856 Patent as well as the requirements added to this claim by claim element 18a.

832. Therefore, at least for the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 18a of the '856 Patent.

833. **Claim 18b: determining that the one or more handshake messages comprise the domain name identified as the network threat.** As detailed below, the Check Point R77 system performs a method that satisfies all requirements of this claim element.

834. As demonstrated above in relation to claim element 1f, the domain name is visible in the handshake message. Furthermore, this domain name can be identified as the network threat.

[178] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.

Hence, the Check Point R77 system performs the method of Claim 1 including determining that the one or more handshake messages comprise the domain name identified as the network threat, as required by claim element 18b.

835. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirement of Claim 1 of the '856 Patent as well as the requirements added to this claim by claim element 18b. Therefore, at least for the reasons above, it is my opinion that the Check Point R77 system anticipates claim element 18b of the '856 Patent.

836. Thus, for at least the reasons above, the Check Point R77 system has been demonstrated to satisfy all requirement of Claim 1 of the '856 Patent as well as all requirements added to this claim by Claim 18 therein.

837. Therefore, at least for the reasons above, it is my opinion that the Check Point R77 system anticipates Claim 18 of the '856 Patent.

4. CLAIM 24

838. **Claim 24a: A packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

839. For at least the reasons detailed in relation to claim element 1a above, the Check Point R77 system includes a packet-filtering system comprised of a hardware processor and memory capable of storing instructions, and when these instruction are executed, the packet-

filtering system receives data indicating a plurality of network-threat indicators, wherein at least one of these indicators comprises a domain name identified as a network threat.

840. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 24a of the '856 Patent.

841. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 24a of the '856 Patent.

842. **Claim 24b: identify packets comprising unencrypted data;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

843. For at least the reasons detailed in relation to claim element 1b above, the Check Point R77 system includes a packet-filtering system capable of identifying packets comprising unencrypted data.

844. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 24b of the '856 Patent.

845. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 24b of the '856 Patent.

846. **Claim 24c: identify packets comprising encrypted data;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

847. For at least the reasons detailed in relation to claim element 1c above, the Check Point R77 system includes a packet-filtering system capable of identifying packets comprising encrypted data.

848. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 24c of the '856 Patent.

849. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 24c of the '856 Patent.

850. **Claim 24d: determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

851. For at least the reasons detailed in relation to claim element 1d above, the Check Point R77 system includes a packet-filtering system capable of determining, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators.

852. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 24d of the '856 Patent.

853. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 24d of the '856 Patent.

854. **Claim 24e: filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of**

network-threat indicators; and As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

855. For at least the reasons detailed in relation to claim element 24e above, the Check Point R77 system includes a packet-filtering system capable of filtering packets, based on data parameters listed in claim element 1e, comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators.

856. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 24e of the '856 Patent.

857. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 24e of the '856 Patent.

858. **Claim 24f: the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

859. For at least the reasons detailed in relation to claim element 1f above, the Check Point R77 system includes a packet-filtering system capable of performing the functionality of claim element 24f.

860. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 24f of the '856 Patent.

861. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 24f of the '856 Patent.

862. **Claim 24g: route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to**

the one or more network-threat indicators. As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

863. For at least the reasons detailed in relation to claim element 1g above, the Check Point R77 system includes a packet-filtering system capable of performing the functionality of claim element 24g.

864. Hence, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 24g of the '856 Patent, and thus the Check Point R77 system anticipates claim element 24g of the '856 Patent.

865. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates each and every element of Claim 24 of the '856 Patent.

5. CLAIM 25

866. **Claim 25a: One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;** The Check Point R77 system includes non-transitory computer-readable media. See analysis of claim element 1a.

867. As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

868. For at least the reasons detailed in relation to claim element 1a above, the Check Point R77 system includes non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to receive data indicating a plurality of network-threat indicators,

wherein at least one of these indicators comprises a domain name identified as a network threat.

869. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 25a of the '856 Patent.

870. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 25a of the '856 Patent.

871. **Claim 25b: identify packets comprising unencrypted data;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

872. For at least the reasons detailed in relation to claim element 1b above, the Check Point R77 system includes non-transitory computer-readable media, as described in relation to claim element 25a, capable of identifying packets comprising unencrypted data.

873. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 25b of the '856 Patent.

874. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 25b of the '856 Patent.

875. **Claim 25c: identify packets comprising encrypted data;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

876. For at least the reasons detailed in relation to claim element 1c above, the Check Point R77 system includes non-transitory computer-readable media, as described in relation to claim element 25a, capable of identifying packets comprising encrypted data.

877. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 25c of the '856 Patent.

878. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 25c of the '856 Patent.

879. **Claim 25d: determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

880. For at least the reasons detailed in relation to claim element 1d above, the Check Point R77 system includes non-transitory computer-readable media, as described in relation to claim element 25a, capable of determining, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators.

881. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 25d of the '856 Patent.

882. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 25d of the '856 Patent.

883. **Claim 25e: filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command**

specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

884. For at least the reasons detailed in relation to claim element 1e above, the Check Point R77 system includes non-transitory computer-readable media, as described in relation to claim element 25a, capable of filtering packets, based on data parameters listed in claim element 25e, comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators.

885. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 25e of the '856 Patent.

886. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 25e of the '856 Patent.

887. **Claim 25f: the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

888. For at least the reasons detailed in relation to claim element 1f above, the Check Point R77 system includes non-transitory computer-readable media, as described in relation to claim element 25a, capable of performing the functionality of claim element 25f.

889. Thus, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 25f of the '856 Patent.

890. Therefore, for at least the reasons given above, it is my opinion that the Check Point R77 system anticipates claim element 25f of the '856 Patent.

891. **Claim 25g: route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.** As detailed below, the Check Point R77 system satisfies all requirements of this claim element.

892. For at least the reasons detailed in relation to claim element 1g above, the Check Point R77 system includes non-transitory computer-readable media, as described in relation to claim element 25a, capable of performing the functionality of claim element 25g.

893. Hence, for at least the reasons above, it is my opinion that the Check Point R77 system satisfies all requirements of claim element 25g of the '856 Patent, and thus the Check Point R77 system anticipates claim element 25g of the '856 Patent.

894. Therefore, for at least the reasons above, it is my opinion that the Check Point R77 system anticipates each and every element of Claim 25 of the '856 Patent.

C. OBVIOUSNESS IN VIEW OF BLUE COAT IN COMBINATION WITH TIPPING POINT IPS

1. BLUE COAT IN COMBINATION WITH TIPPING POINT

895. The Blue Coat SV800 Secure Socket Layer (SSL) Visibility Appliance (Blue Coat SV800) performs the function of filtering and unencrypting SSL traffic, and the TippingPoint Unity One-200 Intrusion Prevention System (IPS) (TippingPoint IPS) performs the function of filtering and logging unencrypted traffic. Thus, the Blue Coat SV800 functions as an SSL proxy, sending certain decrypted packets for inspection against a set of security rules by TippingPoint. Therefore, in the event that the '856 Patent is correctly interpreted to require a separate proxy device, contrary to Plaintiffs' infringement contentions regarding Vision

ONE, Blue Coat SV800 in conjunction with TippingPoint satisfy all requirements of the asserted claims therein.

896. The Blue Coat SV800 SSL Visibility Appliance was commercially available to purchase before December 23, 2015, and the TippingPoint Unity One-200 IPS was commercially available to purchase in 2005. Material showing the availability of the Blue Coat appliance includes the following:

a. The Blue Coat SV800 and SV1800 Getting Started Guide, version 3.8, notes a document revision date of 09/19/14 and a copyright date of ©2014. (SV800_SV1800_GettingStartedGuide_3.8.pdf); also available at https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10256/en_US/SV800_SV1800_GettingStartedGuide_3.8.pdf?__gda__=1532593048_4b7df810810e4aa9bbad21b8e4cb32de.

b. On May 20, 2015, Softpedia News published an article discussing Blue Coat's SSL Visibility appliances, including discussion of the SV800 model. May 30 2015 Softpedia News Article, Blue Coat Patches SSL Visibility Appliance Against 4 Security Bugs (https://news.softpedia.com/news/Blue-Coat-Patches-SSL-Visibility-Appliance-Against-4-Security-Bugs-482776.shtml).

c. https://www.youtube.com/watch?v=IzMhm10ZWs4

897. An illustration of how the Blue Coat SV800 and TippingPoint IPS fit into a typical network architecture is shown in Figure 174[179]. In this configuration, the Blue Coat device acts as an SSL proxy, and directs decrypted packets to the TippingPoint IPS, which constitutes the "Active security device," for inspection against network security rules.

[179] SSL Visibility 3.x First Steps WebGuide: Deployment Modes Overview, https://origin-symwisedownload.symantec.com/resources/webguides/sslv/sslva_first_steps/Content/Topics/Overviews/deployment_modes_overview.htm, accessed 7/26/2018

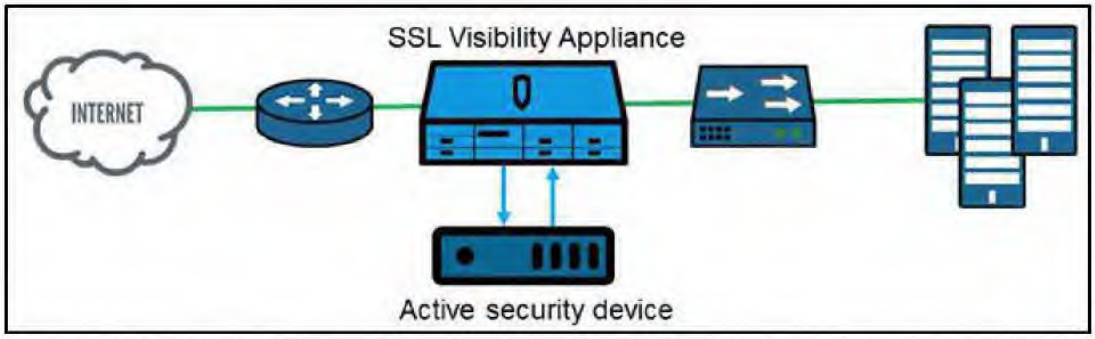


Figure 174: Blue Coat/TippingPoint setup, using the "Active-Inline" configuration. The Blue Coat SV1800 is the "SSL Visibility Appliance" and the TippingPoint IPS is the "Active Security Device".

2. MOTIVATION TO COMBINE

898. A POSITA would recognize that a typical usage case for the Blue Coat SV800 would be in conjunction with a packet broker or IPS device such as TippingPoint IPS. For example, the Blue Coat SV800 instruction manual mentions that the device was designed to work alongside existing security devices such as an IPS[180].

> The SSL Visibility Appliance is designed to work alongside existing security devices such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Data Loss Prevention systems (DLP), Network Forensic appliances, and so on. It provides a non encrypted version of SSL traffic to the associated appliance while maintaining an end to end SSL connection between the client and server involved in the session.

Figure 175: Excerpt from Blue Coat SV800 manual

899. POSITAs taught the use of the Blue Coat SV800 with IPS devices such as the TippingPoint IPS, including as shown during the youtube video published by Angelo's IT Security Channel on February 25, 2016. https://www.youtube.com/watch?v=tCWA-JKa1SU&t=464s.

900. The Blue Coat SV800 can function to decrypt SSL packets, such that they may be inspected by an IPS, and can also be configured to reject certain packets based on broad

[180] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 3

filters so as to prevent certain unwanted traffic, which will ultimately be rejected, from having to be inspected by the IPS. Thus, a POSITA would recognize the benefit of placing a Blue Coat SV800 in conjunction with a Tipping Point IPS is at least twofold: (1) the Blue Coat enables previously encrypted packets to be inspected and filtered according to the rules of the IPS; and (2) the IPS does not need to apply its filtering, which may be more nuanced and computationally complex than the rejection filters of the Blue Coat, to all traffic, but rather only to traffic which isn't clearly unwanted.

901. The Blue Coat and IPS combination relies on the substitution or incorporation of elements that were known in the prior art, as described in the references themselves as well as in earlier published patent and non-patent literature; for example, in United States patent application publication No US 2012/0304224 ("Xie") titled "Malware Analysis System" (filed on May 24 2011 and published on November 29, 2012). Figure 1 of Xie, reproduced below in Figure 176, shows the use of an SSL/SSH decrypt engine (110) being used in conjunction with a policy check engine in a firewall (106), which further evidences an awareness among POSITAs that an SSL proxy system can be used in conjunction with an intrusion prevention system. Also, the combination of the familiar elements claimed in the '856 patent according to known methods or systems would have been obvious because it does no more than yield predictable results. A person of ordinary skill in the art would have been motivated to combine or adapt these known methods or systems. The Blue Coat and IPS combination offers what is asserted and claimed in the '856 patent to constitute improvements over the prior art.

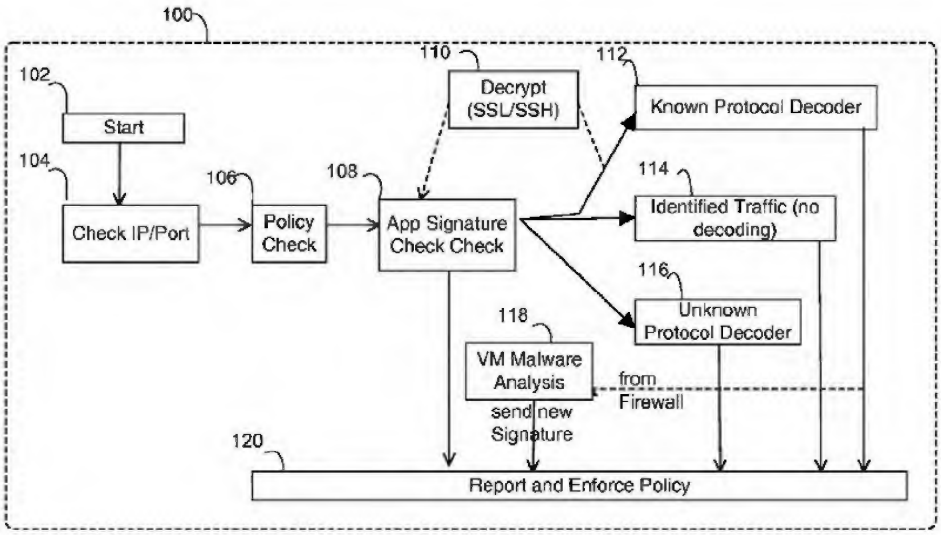


Figure 176: Fig. 1 of Xie.

902. Therefore, at least because the typical usage case of a Blue Coat is as an SSL proxy in conjunction with an IPS, it is my opinion that a POSITA would have been able to make this combination, and would have had a reasonable expectation of success without undue experimentation; and, at least because of the benefits that this combination provides, it is my opinion that a POSITA would have been motivated to make such a combination.

3. CLAIM 1

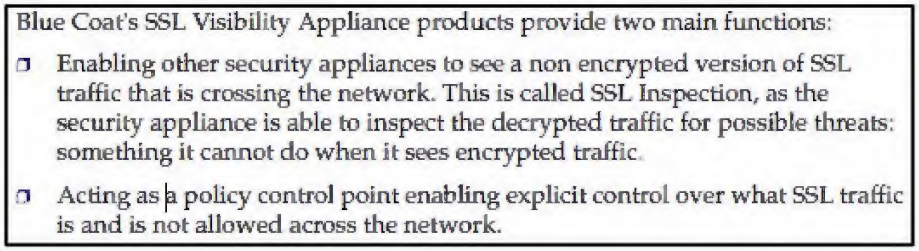
903. **Claim 1a: A method comprising: receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

904. The '856 Patent specification makes many references to a "packet-filtering system," but provides no explicit definition of this term. It is my understanding that no claim construction has been submitted for the term "packet filtering system," with respect to the '856 Patent, and thus the plain and ordinary meaning should be applied. However, it is also my understanding that there was a dispute regarding the construction of a similar term in the Joint Claim Construction Statement[181] with respect to the '722 Patent. While I have applied the plain and ordinary meaning to the term "packet filtering system" for the '856 Patent, because the '722 and '856 Patents have similar specifications, with similar or identical terms in the claim language, and address similar subject matters at similar points in time as would be understood by a similar POSITA, I have also considered the respective claim constructions addressed in the Joint Claim Construction Statement while performing my analysis herein.

905. I understand that in relation to the '722 Patent there is a dispute regarding the construction of the term "packet-filtering device." More specifically, Plaintiffs have proposed that this term be construed as "a device programmed to filter packets based on data associated with a packet," while Defendants have proposed that no construction is needed and that this term should be given its "plain meaning." I have considered both proposed constructions of the term "packet-filtering system," per the similar term in the Joint Claim Construction Statement, as well as the plain an ordinary meaning of this term as would have been understood by a POSITA at the time of the invention, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Blue Coat and the TippingPoint systems each comprise a "packet-filtering system," as explained below.

[181] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))

906. The Blue Coat SV800 performs two main functions, as described in the excerpt below[182]:


Blue Coat's SSL Visibility Appliance products provide two main functions:

- Enabling other security appliances to see a non encrypted version of SSL traffic that is crossing the network. This is called SSL Inspection, as the security appliance is able to inspect the decrypted traffic for possible threats: something it cannot do when it sees encrypted traffic.
- Acting as a policy control point enabling explicit control over what SSL traffic is and is not allowed across the network.

Figure 177: Excerpt from Blue Coat SV800 manual.

907. Similarly, the '856 Patent specification makes many references to "packet-filtering rules," but again provides no explicit definition of this term. I understand that in relation to the '856 Patent there is a dispute regarding the construction of the term "packet-filtering rules." More specifically, Plaintiffs have proposed that this term be construed as "condition or set of conditions that when satisfied cause a computing device to filter packets based on data associated with a packet," while Defendants have proposed "(i) packet-identifying criteria and (ii) an operator to be performed on the identified packets." I have considered both proposed constructions of this term in my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Blue Coat system each receives "a plurality of packet-filtering rules," as detailed below.

908. A plurality of packet-filtering rules can be implemented using the Blue Coat SV800Packet-filtering rules (policies) are available in the Blue Coat SV800 and can include the following elements[183]:

[182] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 3
[183] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 21

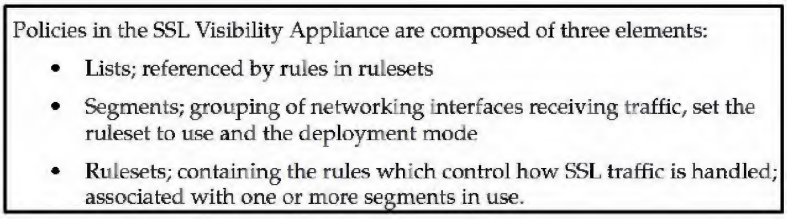


Figure 178: Excerpt from Blue Coat SV800 manual.

909. As with the terms "packet-filtering system" and "packet-filtering rules," the '856 Patent specification makes many references to "network-threat indicators," as a means of filtering transmitted packet information, but does not define what constitutes a "network-threat indicator. I understand that the parties have agreed that the term "network-threat indicators" is to be construed as "indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like." I have applied this construction throughout my analysis, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. In any event, the Blue Coat system comprises a method which includes "network-threat indicators" indicated by data received from the packet filtering system, in accord with the associated packet filtering rules, as required by this claim element.

910. Lists can handle domains identified as a network threat, as is described in the "lists" section of the Blue Coat SV800 manual[184]:

[184] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 21

Lists are used to collect multiple items of the same type of information so that a single ruleset can point to the list and will be applied whenever any of the items in the list are true. For example, a list may contain 20 different Subject/Domain Names (S/DN) that occur in the server certificates from 20 different sites, a policy that is configured to "inspect" traffic when it detects a particular Subject/Domain Name can point to the list instead of just indicating a single Domain Name in the policy. This allows a single policy entry to apply to all 20 different sites and means that additional sites can be added (by editing the list) without needing to edit the ruleset.

Figure 179: Excerpt from Blue Coat SV800 manual.

911. Furthermore, Blue Coat SV800 is able to analyze specifics of a domain, as is shown in the excerpt below.[185]

The SSL Visibility Appliance extracts CN, Subject Alternative Name (SAN), and Server Name Indication (SNI) information from intercepted flows in order to deduce the SSL server domain name. The SSL flows are matched against rules using this process:

1. The SSL Visibility Appliance policy rules support the following subject distinguished name (DN) attributes:
    - CN: Common Name
    - O: Organization
    - OU: Organizational Unit
    - C: Country

Figure 180: Sample SSL rules

912. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 1a of the '856 Patent.

913. **Claim 1b: identifying packets comprising unencrypted data;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

914. The Blue Coat system automatically identifies and "cuts through" non-SSL and non-TLS (collectively referred to as "non-SSL") traffic[186]:

[185] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 23

[186] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 5

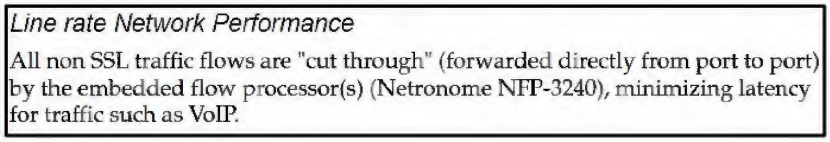


Figure 181: Excerpt from Blue Coat SV800 manual.

915. Therefore, the Blue Coat SV1800 identifies packets comprising unencrypted data. Furthermore, TLS traffic such as the TLS handshake is additional unencrypted data that can be identified by the Blue Coat system, as described in the analysis of claim 1c below.

916. Therefore, for at least the reasons above, it is my opinion that the combined abilities of the Blue Coat and TippingPoint system satisfy claim element 1b of the '856 Patent.

917. **Claim 1c: identifying packets comprising encrypted data;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

918. Encrypted data is automatically identified by Blue Coat, as described by the manual[187]:

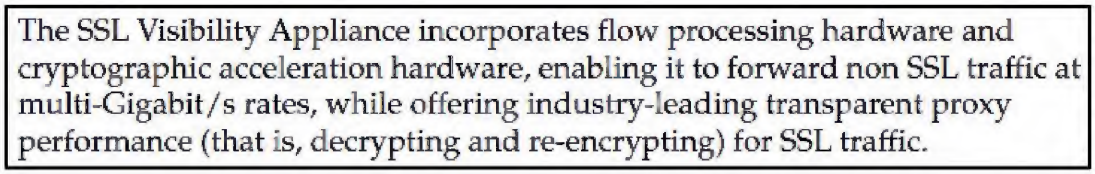
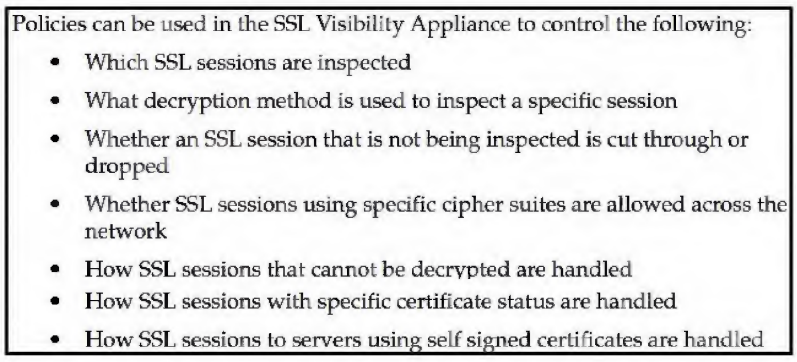


Figure 182:Excerpt from Blue Coat SV800 manual

919. Multiple policies for encrypted data can be implemented within the system[188]

[187] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 3
[188] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 21


Policies can be used in the SSL Visibility Appliance to control the following:

- Which SSL sessions are inspected
- What decryption method is used to inspect a specific session
- Whether an SSL session that is not being inspected is cut through or dropped
- Whether SSL sessions using specific cipher suites are allowed across the network
- How SSL sessions that cannot be decrypted are handled
- How SSL sessions with specific certificate status are handled
- How SSL sessions to servers using self signed certificates are handled

Figure 183: Excerpt from Blue Coat SV800 manual

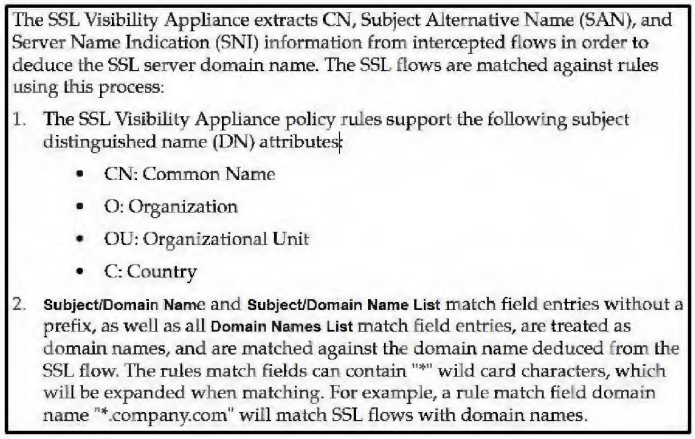
920. The identification of SSL (or TLS) sessions along with the identification of information such as cipher suites and certificates implies the identification of unencrypted data along with the identification of encrypted data.

921. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 1c of the '856 Patent.

922. Claim 1d: determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators; As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

923. Blue Coat is able to use a portion of the unencrypted data to inspect packets for network threat indicators. The excerpt below presents these capabilities.[189]

[189] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 23



The SSL Visibility Appliance extracts CN, Subject Alternative Name (SAN), and Server Name Indication (SNI) information from intercepted flows in order to deduce the SSL server domain name. The SSL flows are matched against rules using this process:

1. The SSL Visibility Appliance policy rules support the following subject distinguished name (DN) attributes:
   - CN: Common Name
   - O: Organization
   - OU: Organizational Unit
   - C: Country
2. **Subject/Domain Name** and **Subject/Domain Name List** match field entries without a prefix, as well as all **Domain Names List** match field entries, are treated as domain names, and are matched against the domain name deduced from the SSL flow. The rules match fields can contain "*" wild card characters, which will be expanded when matching. For example, a rule match field domain name "*.company.com" will match SSL flows with domain names.

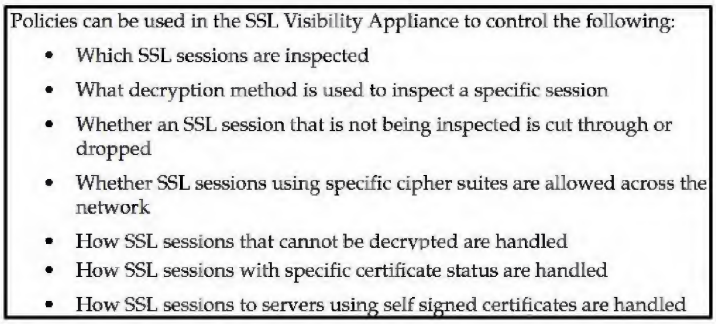
Figure 184: Excerpt from Blue Coat SV800 manual

924. For example, the SNI is an unencrypted section of the TLS handshake that specifies the domain name of the server being contacted. This information can also be found in the certificate sent back subsequently by the server.

925. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 1d of the '856 Patent.

926. **Claim 1e: filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and** As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

927. Blue Coat is capable of multiple filtering techniques, and policies for the filtering are described in the manual[190]:


Policies can be used in the SSL Visibility Appliance to control the following:

- Which SSL sessions are inspected
- What decryption method is used to inspect a specific session
- Whether an SSL session that is not being inspected is cut through or dropped
- Whether SSL sessions using specific cipher suites are allowed across the network
- How SSL sessions that cannot be decrypted are handled
- How SSL sessions with specific certificate status are handled
- How SSL sessions to servers using self signed certificates are handled

Figure 185: Excerpt from Blue Coat SV800 manual

928. For example, one example of "data indicating a method specified by a plurality of packet-filtering rules" is "What decryption method is used to inspect a specific session".

929. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 1e of the '856 Patent.

930. **Claim 1f: the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and** As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

931. Packets that are identified can be filtered in multiple ways (including cut through, dropped, or rejected), as is shown in the excerpt below[191]:

[190] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 21
[191] Blue Coat Systems SV800 & SV1800-C/F Administration & Deployment Guide, Software: V. 3.8.0, Document Revision 9/22/2014, Page 29

Table 8 shows details for Cut Through/Drop/Reject rules that will trigger actions other than decryption, for example rules that cut sessions through, reject sessions or drop them if the details in the server certificate for a session match the rule. Some of the match fields can point to lists which allows a single rule entry to be triggered by more than one set of matching criteria.

Table 8 Non-Decryption Format Rules

Item	Default Setting	Notes
Cut Through/Drop/Reject		Actions are cut, reject or drop

(Table truncated)

Figure 186: Excerpt from Blue Coat SV800 manual

932. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 1f of the '856 Patent.

933. **Claim 1g: routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators** As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

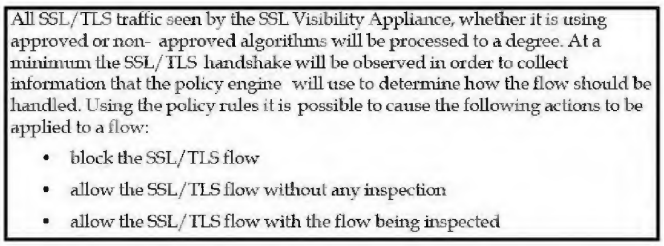
934. I understand there is a dispute regarding the construction of the term "proxy system," in relation to the '856 Patent. More specifically, in the Joint Claim Construction Statement[192] Plaintiff has proposed that this term be given its plain and ordinary meaning, while Defendants have proposed that this term be construed as a "system that establishes connections to devices in trusted and untrusted environments and relays packets between a device in the trusted environment and a device in the untrusted environment".[193] I have

[192] Joint Claim Construction and Prehearing Statement (No. 2:17-cv-00383 (HCM-LRL))
[193] *See* Joint Claim Construction And Prehearing Statement, Exhibit 2.

considered both proposed constructions in my analysis in addition to the description of this term within the '856 Patent specification, and I reserve the right to amend this analysis should the Court rule that a different construction should be applied. Regardless of which construction is applied, the Blue Coat SV800 satisfies all requirements of this claim element, for at least the reasons detailed below.

935. Blue Coat SV800 is capable of routing all of its packets to an IPS (such as the TippingPoint Unity One-200 IPS). The TippingPoint IPS is a proxy system that is capable of logging unencrypted packets.

936. The exceprt below shows a description of how the Blue Coat SV800 is capable of handling SSL/TLS trafic[194].


All SSL/TLS traffic seen by the SSL Visibility Appliance, whether it is using approved or non- approved algorithms will be processed to a degree. At a minimum the SSL/TLS handshake will be observed in order to collect information that the policy engine will use to determine how the flow should be handled. Using the policy rules it is possible to cause the following actions to be applied to a flow:

- block the SSL/TLS flow
- allow the SSL/TLS flow without any inspection
- allow the SSL/TLS flow with the flow being inspected

Figure 187: Excerpt from FIPS 140-2 Non-Proprietary Security Policy.

937. "Inspection" in Figure 187 refers to Blue Coat SV800 unencrypting the packet, thus enabling another security device to inspect the unencrypted packet[195]:

[194] Blue Coat Systems SSL Visibility Appliance: FIPS 140-2 Non-Proprietary Security Policy, Models SV1800-C, SV1800-F, SV 2800, Firmware Version 3.8.4, Document Revision 8/10/2015, page 13
[195] Blue Coat Systems SSL Visibility Appliance: FIPS 140-2 Non-Proprietary Security Policy, Models SV1800-C, SV1800-F, SV 2800, Firmware Version 3.8.4, Document Revision 8/10/2015, page 9

> Blue Coat's SSL Visibility Appliance products provide two main functions when deployed within a network:
>
> - They enable other security appliances to see a non encrypted version of SSL/TLS traffic that is crossing the network. This is called SSL Inspection.
> - They can act as a policy control point enabling explicit control over what SSL/TLS traffic is and is not allowed across the network.

Figure 188: Excerpt from FIPS 140-2 Non-Proprietary Security Policy.

938. If the Blue Coat S800 inspects (i.e., unencrypts) a malicious packet, the unencrypted packet can be sent to the TippingPoint IPS, which is capable of capturing unencrypted packets. The TippingPoint IPS can be programmed to capture packets based on a variety of filters, a sampling of which is shown in the figure below.

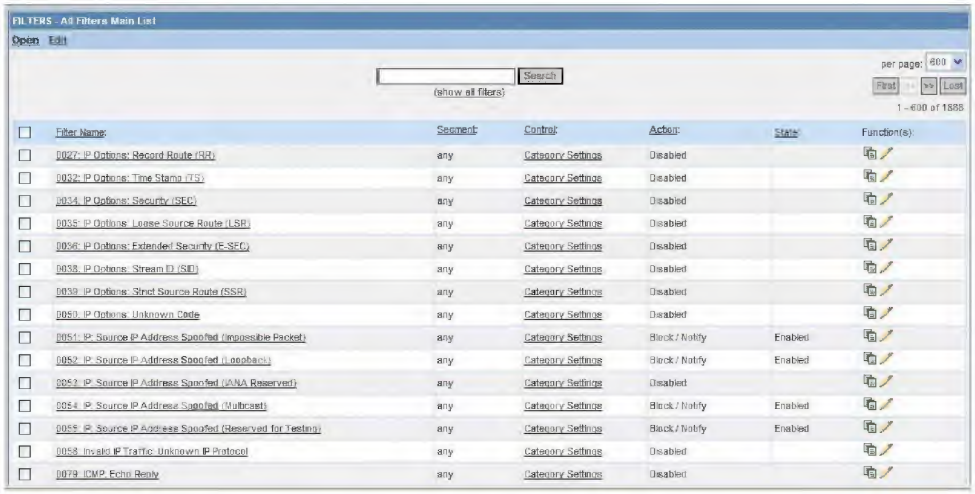


Figure 189: Example Filters for TippingPoint IPS

939. The TippingPoint IPS, which can be connected to the Blue Coat SV800 as the Active Security Device as seen in Figure 174, is capable of inspecting, filtering, and logging unencrypted packets, as is illustrated in the LSM Users Guide[196]:

[196] TippingPoint UnityOne Local Security Manager User's Guide, Version 2.1, Copyright 2005, Page 100

CENTRIPETAL-CSCO 087840

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 340

Action Name	Description
Block + Notify + Trace (+TCP Reset) (+Blacklist)	Blocks a packet from being transferred, notifies all selected contacts of the blocked packet, and logs all information about the packet according to the packet trace settings. TCP Reset is an option for resetting blocked TCP flows. Blacklist is an option that blocks traffic based on IP addresswhen the filters triggers, adding it to a list of blocked IPs.

Figure 190: Packet logging capability of TippingPoint IPS

Further information regarding the packet information recorded by TippingPoint IPS is also provided in the manual[197]:

- **Packet Trace** — allows you to capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.
  - — **Priority** — sets the relative importance of the information captured. Low priority items will be discarded before medium priority items if there is a resource shortage.
  - — **Verbosity** — determines how much of a suspicious packet will be logged for analysis. If you choose *full* verbosity, the whole packet will be recorded. If you choose *partial* verbosity, you can choose how many bytes of the packet (from 64 to 1600 bytes) the packet trace log records.

Figure 191: Packet Trace and logging

[197] TippingPoint UnityOne Local Security Manager User's Guide, Version 2.1, Copyright 2005, Page 100

CENTRIPETAL-CSCO 087841

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 341

Packets that are blocked by the TippingPoint IPS are displayed in a "Block Log"

Block Log

The Block log contains information about packets that have triggered a filter with both block and alert actions specified. The Block Log entries include the following information:

Table 4 - 2: Block Log Information

Column	Description
Log ID	A system assigned Log ID number
Date/Time	A date and time stamp in the format year-month-date hour:minute:second
Severity	Indicates the severity of the triggered filter. Possible values include: Critical, Major, Minor, and Low
Filter Name	The name of the filter that was triggered
Protocol	The name of the protocol that the action affects
Segment	The segment where the alert occurred
Source Address	The source address of the triggering traffic
Dest Address	The destination address of the triggering traffic
Packet Trace	Details if a packet trace is available
Hit Count	Details how many packets have been detected

Figure 192: Block Log details

940. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 1g of the '856 Patent.

941. Consequently at least the reasons detailed above, it is my opinion that Blue Coat in combination with TippingPoint satisfies each and every limitation of claim 1 of the 856 Patent. Consequently, for at least the reasons above, it is my opinion that claim 1 of the '856 Patent is rendered obvious by this combination.

4. CLAIM 18

942. **Claim 18a: The method of claim 1, wherein the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:** As detailed below, the combined abilities of the

CENTRIPETAL-CSCO 087842

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 342

Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

943. I understand that the parties have agreed that the term "handshake messages" is to be construed as "messages to establish a session or connection,"[198] and I have applied this construction throughout my analysis herein.

944. An SSL connection requires a transfer of unencrypted "handshake" packets in order to establish a secure connection. Claim 1d explains the different filtering techniques that can occur with the Blue Coat SV800 device.

945. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 18a of the '856 Patent.

946. **Claim 18b: determining that the one or more handshake messages comprise the domain name identified as the network threat.** As detailed below, the combined abilities of the Blue Coat and TippingPoint system perform a method that satisfies all requirements of this claim element.

947. The "Client hello" in the SSL handshake is an example of an "SNI" parameter, which Blue Coat SV800 is capable of detecting. See claim element 1d.

948. Therefore, for at least the reasons above, it is my opinion that the combined abilities of the Blue Coat and TippingPoint system satisfy claim element 18b of the '856 Patent.

949. Consequently at least the reasons detailed above, it is my opinion that the Blue Coat system satisfies each and every limitation of claim 18 of the '856 Patent. Consequently, for at least the reasons above, it is my opinion that claim 18 of the '856 Patent is obvious by the combined abilities of the Blue Coat and TippingPoint system.

---

[198] *See* Joint Claim Construction And Prehearing Statement, Exhibit 1.

5. CLAIM 24

950. **Claim 24a: A packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

951. See analysis of claim element 1a

952. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 24a of the '856 Patent.

953. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 24a of the '856 Patent.

954. **Claim 24b: identify packets comprising unencrypted data;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

955. See analysis of claim element 1b.

956. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 24b of the '856 Patent.

957. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 2ba of the '856 Patent.

958. **Claim 24c: identify packets comprising encrypted data;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

959. See analysis of claim element 1c.

960. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 24c of the '856 Patent.

961. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 24c of the '856 Patent.

962. **Claim 24d: determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

963. See analysis of claim element 1d.

964. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 24d of the '856 Patent.

965. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 24d of the '856 Patent.

966. **Claim 24e: filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by**

the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and As detailed below, the Blue Coat system performs a method that satisfies all requirements of this claim element.

967. See analysis of claim element 1e.

968. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 24e of the '856 Patent.

969. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 24e of the '856 Patent.

970. **Claim 24f: the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

971. and See analysis of claim element 1f.

972. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 24f of the '856 Patent.

973. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 24f of the '856 Patent.

974. **Claim 24g: route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

975. See analysis of claim element 1g.

976. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 24g of the '856 Patent.

977. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 24g of the '856 Patent.

Consequently at least the reasons detailed above, it is my opinion that Blue Coat in combination with TippingPoint satisfies all limitations of all elements of claim 24 of the '856 Patent; and thus, for at least the reasons above, it is my opinion that claim 24 of the '856 Patent is obvious in view of this combination.

6. CLAIM 25

978. **Claim 25a: One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

979. The combined abilities of the Blue Coat and TippingPoint system includes non-transitory computer-readable media. See analysis of claim element 1a.

980. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 25a of the '856 Patent.

981. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 25a of the '856 Patent.

982. **Claim 25b: identify packets comprising unencrypted data;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

983. See analysis of claim element 1b.

984. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 25b of the '856 Patent.

985. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 25b of the '856 Patent.

986. **Claim 25c: identify packets comprising encrypted data;** As detailed below, the Blue Coat system performs a method that satisfies all requirements of this claim element.

987. See analysis of claim element 1c.

988. Thus, for at least the reasons detailed above, the Blue Coat system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 25c of the '856 Patent.

989. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 25c of the '856 Patent.

990. **Claim 25d: determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

991. See analysis of claim element 1d.

992. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 25d of the '856 Patent.

993. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 25d of the '856 Patent.

994. **Claim 25e: filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and** As detailed below, the combined abilities of

the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

995. See analysis of claim element 1e.

996. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 25e of the '856 Patent.

997. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 25e of the '856 Patent.

998. **Claim 25f: the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

999. See analysis of claim element 1f.

1000. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 25f of the '856 Patent.

1001. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 25f of the '856 Patent.

1002. **Claim 25g: route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.** As detailed below, the combined abilities of the Blue Coat and TippingPoint system performs a method that satisfies all requirements of this claim element.

1003. See analysis of claim element 1g.

1004. Thus, for at least the reasons detailed above, the combined abilities of the Blue Coat and TippingPoint system constitutes a system that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 25g of the '856 Patent.

1005. Therefore, for at least the reasons above, it is my opinion that Blue Coat in combination with TippingPoint satisfies claim element 25g of the '856 Patent.

1006. Consequently at least the reasons detailed above, it is my opinion that Blue Coat in combination with TippingPoint satisfies each and every limitation of claim 25 of the 856 Patent; and thus, for at least the reasons above, it is my opinion that claim 25 of the '856 Patent is rendered obvious in view of this combination.

XV. U.S. PATENT NO. 9,560,077

1007. I have been asked to review the '077 Patent and assess the validity of Claims 7 and 13. First, I will summarize the '077 patent briefly and then discuss claim-by-claim invalidity analysis.

A. SUMMARY OF THE '077 PATENT

1008. The '077 patent assigned to Centripetal Networks, Inc., Herndon, VA (US), was filed on Apr. 28, 2015 and published on Jan. 31, 2017. This patent was a continuation of application No. 13/657,010, which was later published as the '205 patent. The '077 patent relates to methods and systems for protecting a secured network. Specifically, it relates to packet filtering of network traffic using security policy management (SPM) servers and packet security gateways (PSGs). [199]

[199] '077 patent, at 1:48-61

1009. A security policy management (SPM) server is a computing device that is configured to communicate a dynamic security policy to a packet security gateway.[200] Figure 193 illustrates an exemplary SPM including memory, processor, management interface, and network interface (NI). The memory in SPM stores various program modules and dynamic security policies, which include criteria corresponding to one or more packets and a packet transformation function to be performed on packets corresponding to the specified criteria.[201] The processor executes program modules to configure SPM to (1) communicate dynamic security policies to PSGs, (2) receive updates from malicious host tracker service, and (3) automatically alter or create one or more rules related to malicious network traffic. The management interface provides administrators access to SPM via a graphical user interface (GUI) or a command line interface (CLI). Administrators can use management interface to add PSGs and to construct new dynamic security policies. The NI interfaces SPM with the network environment and facilitates communication between SPM and PSGs.[202]

[200] '077 Patent, at 4:53-55.
[201] '077 patent, at 4: 58-63.
[202] '077 patent, at 13:5 - 14:20

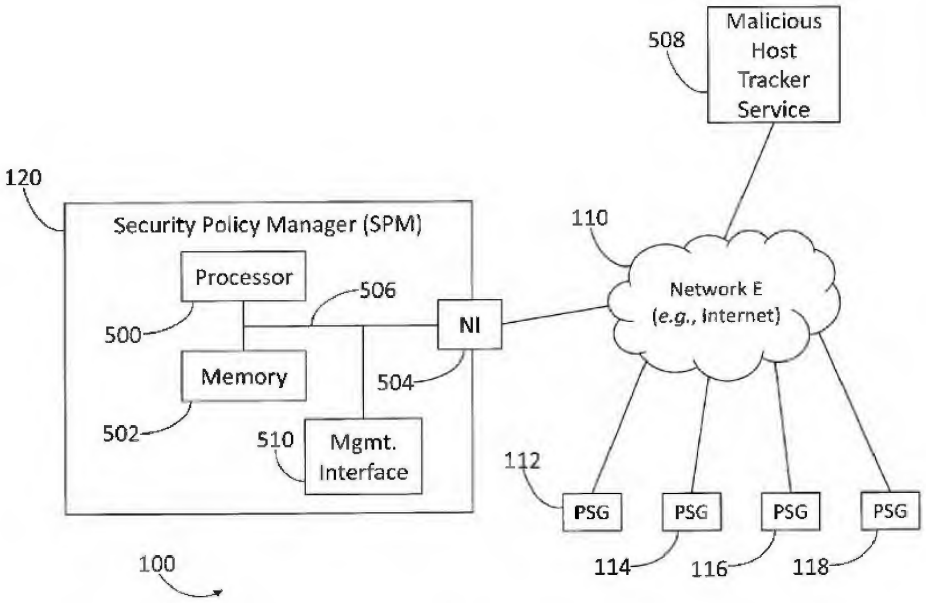


FIG. 5

Figure 193. An exemplary security policy manager (SPM) disclosed in the '077 patent ('077 Patent, FIG. 5).

1010. A packet security gateway is a computing device configured to receive packets and perform a packet transformation on the packets.[203] Figure 194 illustrates an exemplary SPG including the following components: processor, memory, NIs, management interface and packet filter. The processor configures SPG by executing one or more program modules included in the memory. PSG receives dynamic security policies from SPM via the management interface or the network interface. Packet filters examine dynamic security policy and information associated with the packets received by PSG. Based on the results of this analysis, packet filters send the packets to one or more packet transformation functions (PTF), e.g., forward or drop.[204]

[203] '077 Patent, at 4:48-50.
[204] '077 Patent, at 5:41-6:31.

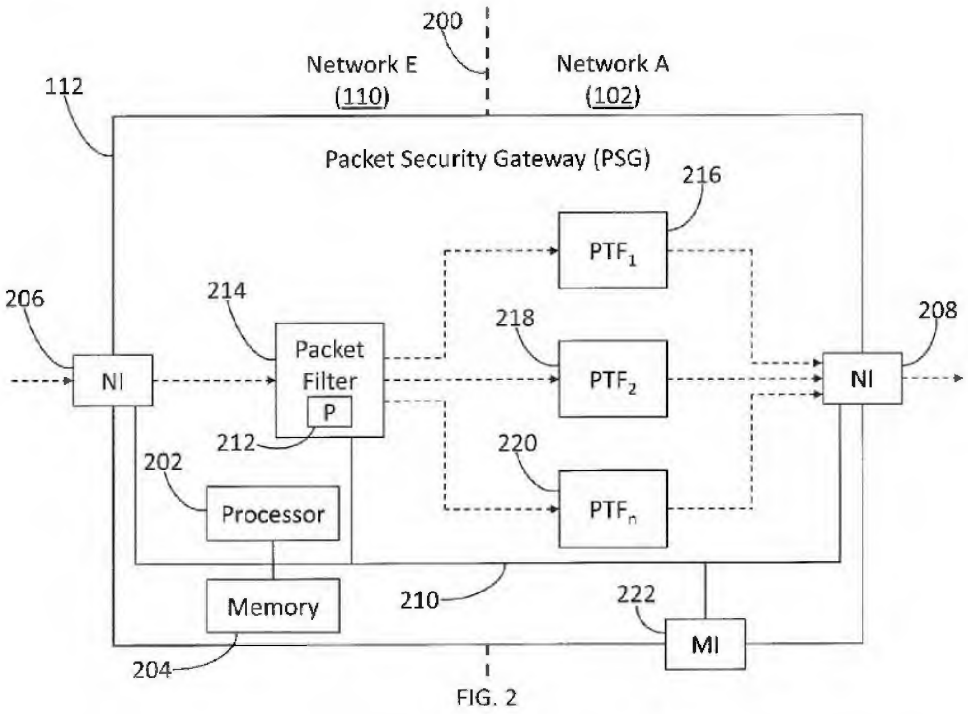


Figure 194. An exemplary packet security gateway (PSG) disclosed in the '077 patent ('077 Patent, FIG. 2).

1011. Figure 195 illustrates an exemplary secure LAN environment including a SPM, a PSG, three hosts, and a LAN switch. LAN switch is configured to switch packets received to/from the hosts. PSG can be either embedded within the LAN switch or a distinct device, in which case LAN switch is directed to route traffic via the PSG. PSG will receive dynamic security policies from SPM regarding packets targeted for the three hosts. Based on the rules in dynamic security policies, SPG performs packet transformation functions on the identified packets and thus, protect the secured LAN environment from network attacks.[205]

[205] '077 patent, at 18:63-19: 38

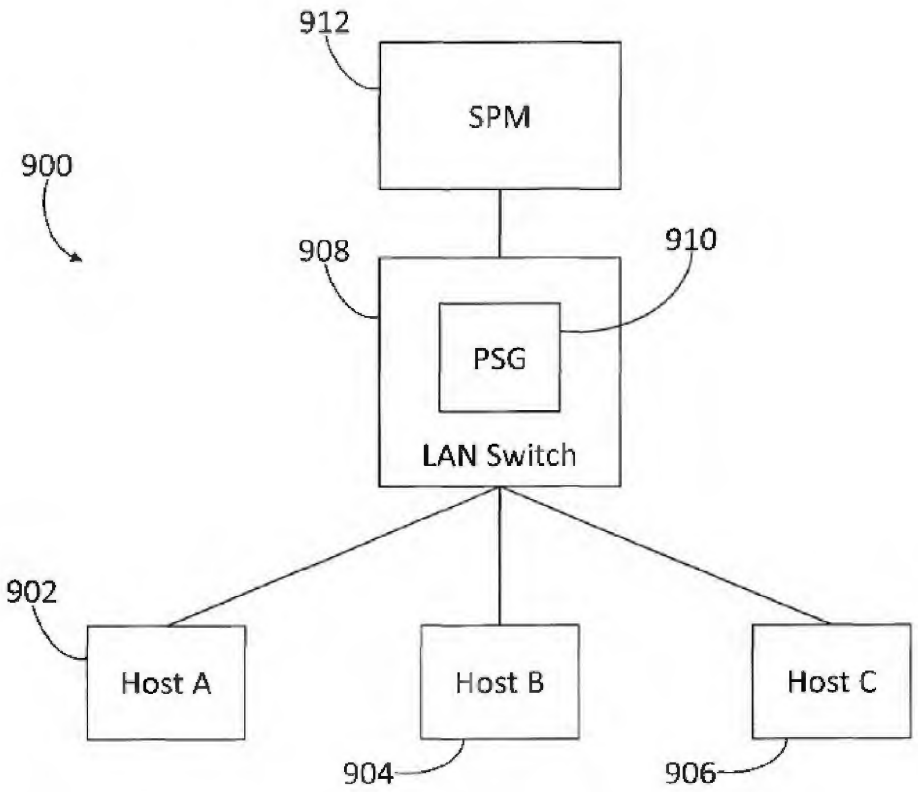


FIG. 9

Figure 195. An exemplary secure LAN environment protected by methods and systems disclosed in the '077 patent ('077 Patent, FIG. 9).

B. ANTICIPATION BY NTO 5236

1. NTO 5236

1012. The Anue Network Tool Optimizer™ NTO 5236 ("NTO 5236") is a network packet broker system for aggregating, filtering, and directing network data to tools such as data recorders, VoIP monitors, or other applications. This system comprises a device with network ports and tool ports. A typical usage case for the system is in a large network where traffic must be routed to many individual tools. The NTO 5236 can filter packets to reduce the load on the tools and balance the packet load among groups of tools.

1013. The NTO 5236 system was commercially available to purchase prior to the priority date of the '077 Patent. The functionality of the NTO 5236 is documented in the NTO 5200 User Guide.[206]

1014. After entering a given network port, packets are forwarded from said network port to the tool ports, where they are filtered again as they leave the system on the tool ports."[207] The NTO 5200 user guide states, "[t]he Anue Net Tool Optimizer (NTO) directs network data from SPAN ports and TAPS in your data center and forwards it to a convenient centralized tool farm where multiple tools can share simultaneous access to the network data."[208]

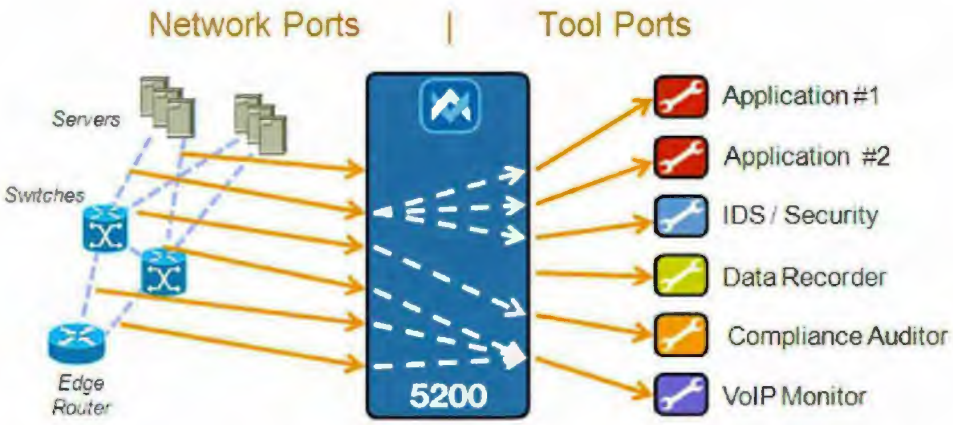


Figure 1-1. Anue NTO Tool Optimization

Figure 196. The NTO 5236, shown in blue, acts as a reconfigurable LAN switch to direct traffic between network ports and tool ports. NTO 5236 user guide, PA0000777

[206] Starting at PA0000777
[207] See NTO 5200 User Guide p. PA0000777
[208] See NTO 5200 User Guide p. PA0000777

1015. The paradigm of the NTO 5236 system is to have span/tap ports within the network and to be able to monitor and record traffic, but not to necessarily block traffic from crossing in or out of the network.

1016. For at least the reasons detailed below, it is my opinion that the NTO 5236 system enabled a person of ordinary skill in the art to practice elements a, b, d, e, f, and g of Claim 7 and elements a, b, d, e, f, and g of Claim 13 of the '077 Patent, and that a POSITA would be motivated to do so as part of the typical routine of setting up the network packet broker. In combination with the TippingPoint IPS, a POSITA would be motivated to practice all elements of Claim 7 and Claim 13.

1017. I understand that Plaintiffs' have accused Vision ONE of infringing upon the '077 Patent. Vision ONE is a packet broker that performs similar functionality as the NTO 5236. More specifically, both Vision ONE and NTO 5236 are directed towards optimized traffic routing, rather than rejecting unwanted packets. Therefore, under Plaintiffs position that Vision ONE infringes upon the asserted '077 Patent, even though Vision ONE does not necessarily reject "bad" packets, the NTO 5236 must necessarily be able to anticipate said claims without rejecting "bad" packets.

2. NTO 5200 User Guide

1018. I was provided with the user guide for the NTO 5236, dated October 2013, as shown in Figure 197. I am informed by counsel that previous user guides are similar to this one.



Anue Net Tool Optimizer 5200 Series
User Guide

NVOS 3.9, October 2013

Figure 197. The title page of the NTO 5236 User Guide, dated October 2013.

1019. I analyzed this user guide to evaluate whether the NTO 5236 system enables a person of ordinary skill in the art to practice the claim elements of the '077 Patent.

3. CLAIM 7

1020. Claim 7a. A system comprising at least one processor. As detailed below, the NTO 5236 system satisfies all requirements of this claim element.

1021. Since the NTO 5236 is a physical computer system, it contains at least one processor.

1022. Therefore, for at least the reasons given above, it is my opinion that the NTO 5236 anticipates claim element 7a of the '077 Patent.

1023. Claim 7b. And a memory storing instructions that when executed by the at least one processor cause the system to. As detailed below, the NTO 5236 system satisfies all requirements of this claim element.

1024. Since the NTO 5236 is a physical computer system, it contains memory[209] that stores instructions that can be executed by the processor.

[209] See NTO 7300 User Guide at PA0000815

1025. Therefore, for at least the reasons given above, it is my opinion that the NTO 5236 anticipates claim element 7b of the '077 Patent.

1026. Claim 7c. Provision, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located. The NTO 5236 system does not explicitly satisfy this claim element because it does not "protect" a network. Unlike for a firewall, not all traffic must pass through the NTO 5236.

1027. **Claim 7d. And configure, each device of the plurality of devices, to.** As detailed below, the NTO 5236 system satisfies all requirements of this claim element.

1028. Several NTO 5236 devices could be used in one network and each device could be configured using the management graphical user interface.[210]

1029. Therefore, for at least the reasons given above, it is my opinion that the NTO 5236 anticipates claim element 7d of the '077 Patent.

1030. **Claim 7e. Receive packets via a communication interface that does not have a network-layer address.** As detailed below, the NTO 5236 system satisfies all requirements of this claim element.

1031. There is no mention of network-layer or IP addresses for the network ports or tool ports in the NTO 5236 user guide. These ports are capable of operating at network layer 2.[211]

1032. Therefore, for at least the reasons given above, it is my opinion that the NTO 5236 anticipates claim element 7e of the '077 Patent.

---

[210] See NTO 7300 User Guide at PA0000777
[211] See NTO 7300 User Guide at PA0000782

1033. Claim 7f. Responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets. As detailed below, the NTO 5236 system satisfies all requirements of this claim element.

1034. As shown in Figure 198, there are three filter types which can drop packets within the NTO 5236: ingress filters, dynamic filters, and egress filters.

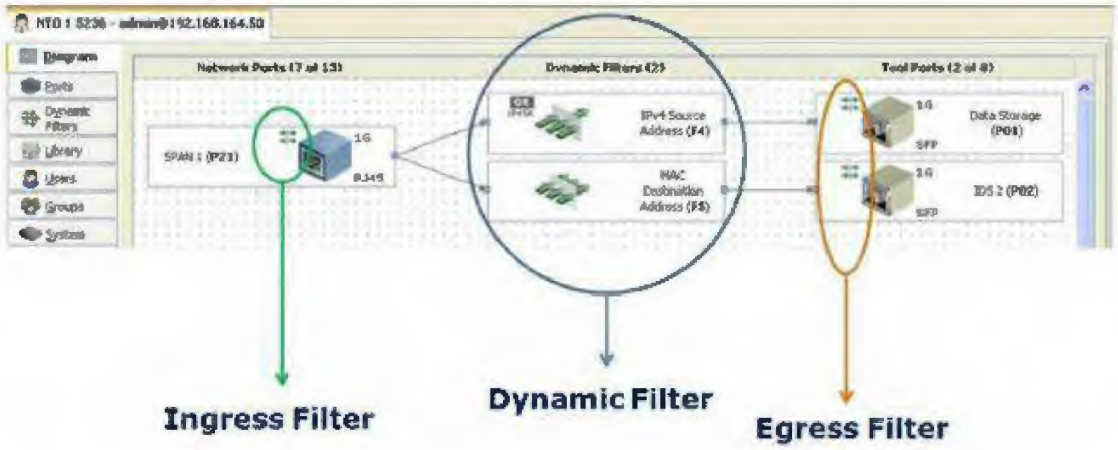


Figure 198. A diagram from the NTO 5236 management graphical user interface showing ingress, dynamic, and egress filters. NTO 5236 user guide, PA0000781.

1035. The user guide states, "Dynamic filters are the primary method used to filter traffic on the Anue NTO."[212] These are the filters that appear in the middle of the NTO 5236 control panel Diagram view. They are optimized for topologies that require both aggregating traffic from multiple network ports to a single tool, as well as sharing traffic from a network port with multiple tools."

[212] See NTO 5200 User Guide at P A0000780

1036. The user's guide continues with: "[i]ngress filters are configured at the network port. Ingress filtering occurs immediately upon traffic entering a network port, upstream from other filter types. One ingress filter can be applied to each network port. "Deny" and "Pass" filter modes are supported. Any traffic that is filtered out (i.e., removed) at ingress is no longer available to any downstream filters or tools;"

1037. Lastly, "[e]gress filters are configured at the tool port. Egress filtering occurs downstream from Ingress and Dynamic filters. "Deny" and "Pass All" filter modes are supported. This filter type is typically used to fine tune filtering in combination with the Dynamic filters. Using a Deny filter to remove traffic that is not required by tools can also improve tool performance." This is an example of "one or more rules, drop[ing] the portion of the packets."

1038. Therefore, for at least the reasons given above, it is my opinion that the NTO 5236 anticipates claim element 7f of the '077 Patent.

1039. **Claim 7g. And modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device.** As detailed below, the NTO 5236 system satisfies all requirements of this claim element.

1040. The NTO 5236, is designed to be connected within a LAN as described above. The NTO 5236 traffic at layer 2 (the layer that a LAN switch operates on) as noted above. Thus, NTO 5236 constitute LAN switches associated with the device.

1041. A deny rule on the NTO 5236 can be included in ingress, egress, and dynamic filters, which causes packets to be dropped. In particular, an operator or user could modify the

dynamic, ingress, or egress filters in order to add a "deny" rule, which would "modify [the] switching matrix" of the NTO 5236.

1042. Furthermore, dynamic filters can filter traffic dynamically, meaning that they can modify the switching matrix of the LAN switch to select which packets should be denied without direct operator or user intervention.

1043. Therefore, for at least the reasons given above, it is my opinion that the NTO 5236 anticipates claim element 7g of the '077 Patent.

4. CLAIM 13

1044. Claim 13 is identical to claim 7, except that claim 7 refers to "a system comprising at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to" execute claim elements 7c through 7g, whereas claim 13 refers to "one or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to" excecute claim elements 13b through 13f, which are identical to claim elements 7c through 7g.

1045. Since the NTO 5236 is a physical computer system as described above, it comprises non-transitory computer-readable media (for example, a hard drive) that stores instructions that are executed by the computing system.

1046. Therefore, for at least the reasons given above, it is my opinion that the NTO 5236 anticipates all elements of claim 13 (except claim 13c) of the '077 Patent.

C. ANTICIPATION AND/OR OBVIOUSNESS IN VIEW OF NTO 5236 AND TIPPINGPOINT IPS

1047. Contrary to Plaintiffs' Infringement Contentions, the '077 Patent does indeed require screening and rejection of packets that match relevant criteria. Under this proper

interpretation the NTO 5236 may be used in combination with an IPS, such as TippingPoint, to satisfy all requirements of the asserted claims therein.

1048. Indeed, the NTO 5236 is designed to be used in conjunction with other security appliances, such as the TippingPoint IPS, and thus such a combination constitutes a typical usage case. More specifically, in such a combination, the NTO 5236 would act as a network packet broker that filters, re-directs, and load distributes traffic before it reaches the TippingPoint IPS. The TippingPoint IPS would be connected to one of the tool ports of the NTO 5236. Hence, the TippingPoint would "protect" the network of claim element 7c and 13c, while the NTO 5236 would act as the reconfigurable LAN switch of claim element 7g and 13g.

1049. Consequently at least the reasons detailed above, it is my opinion that the NTO 5236 in combination with TippingPoint satisfies each and every limitation of claim 7 and claim 13 of the '077 Patent. Therefore, for at least the reasons above, it is my opinion that claim 1 of the '077 Patent is rendered obvious by this combination.

D. LACK OF WRITTEN DESCRIPTION

1050. I understand that Claim 7 recites a limitation that requires "a memory storing instructions that when executed by the at least one processor cause the system to … modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device" (the '077 Patent, Claim 7). Likewise, I understand that Claim 13 recites a limitation that requires "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to … modify a switching matrix of a local area network (LAN) switch associated with the device such that

the LAN switch is configured to drop the portion of the packets responsive to the determination by the device."

1051. These limitations are not described by the '077 Patent specification. Rather, the only disclosure in the '077 Patent specification regarding a "switching matrix" is provided in two paragraphs with respect to Figure 9:

> FIG. 9 illustrates an exemplary secure LAN environment protected in accordance with one or more aspects of the disclosure. Referring to FIG. 9, network environment 900 may be a LAN, including hosts A 902, B 904, and C 906. It may also include LAN switch 908. LAN switch 908 may be configured to switch network traffic (e.g., packets) between one or more of hosts A 902, B 904, and C 906. For example, LAN switch 908 may include a switching matrix configured to switch packets received from one or more of hosts A 902, B 904, and C 906 to one or more of hosts A 902, B 904, and C 906. LAN switch 908 may be associated with packet security gateway 910, and network environment 900 may include security policy management server 912.
>
> In some embodiments, packet security gateway 910 may be embedded within LAN switch 908. Alternatively, packet security gateway 910 may be a device distinct from LAN switch 908, and LAN switch 908 may be configured to route network traffic through packet security gateway 910 (e.g., by modifying LAN switch 908's switching matrix). Packet security gateway 910 may be configured to receive one or more dynamic security policies from security policy management server 912. The dynamic security policies received from security policy management server 912 may include one or more rules specifying criteria associated with one or more of hosts A 902, B 904, and C 906, and may further specify one or more packet transformation functions to be performed on packets matching the specified criteria. Packet security gateway 910 may identify packets matching one or more of the criteria specified by the rules and may perform the associated packet transformation functions on the identified packets. By utilizing packet security gateway 910 within network environment 900, an operator of network environment 900 may be able to protect network environment 900 from network attacks, as

well as implement one or more services (e.g., blocklist service, allowlist service, VoIP firewall service, phased restoration service, enqueueing service, multi-dimensional routing service, or monitoring service) within network environment 900. Network environment 900 may include multiple LAN switches with embedded or associated packet security gateways, each of the packet security gateways configured to receive one or more dynamic security policies from security policy management server 912. ('077 Patent, at 18:63-19:38, emphasis added).

Figure 9, to which these two paragraphs refer, does not illustrate the "switching matrix":

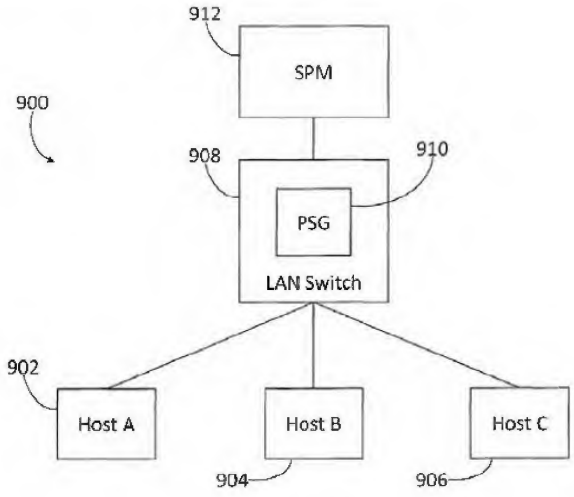


FIG. 9

('077 Patent, Fig. 9.)

1052. The disclosure of the '077 Patent specification in these two paragraphs regarding the "switching matrix" ('077 Patent, at 18:63-19:38) does not provide written description support for the claim terms that recite a "switching matrix." In particular, Claims 7 and 13 each require that computer "instructions" are executed to "modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device." '077 Patent, at Claims 7 and 13 (emphasis added). However, nowhere does the '077 Patent

suggest that a switch matrix is modified to cause a LAN switch to drop any packets. For example, in the first paragraph that mentions a "switching matrix," the '077 Patent specification indicates that "LAN switch 908 may include a switching matrix configured to switch packets received from one or more of hosts A 902, B 904, and C 906 to one or more of hosts A 902, B 904, and C 906" (the '077 Patent, 19:2-6, emphasis added). Thus, the described function of the "switching matrix" is not dropping packets, but rather routing the packets to specified hosts—namely, "one or more of hosts A 902, B 904, and C 906." *Id.* In fact, a POSITA would understand that the packets being routed to specified hosts indicates that the switching matrix does *not* cause packets to be dropped for those specified hosts.

1053. In the second paragraph that mentions a "switching matrix," the '077 Patent specification indicates that "packet security gateway 910 may be a device distinct from LAN switch 908, and LAN switch 908 may be configured to route network traffic through packet security gateway 910 (e.g., by modifying LAN switch 908's switching matrix)" (the '077 Patent, 19:10-14). However, the LAN switch 908 being configured to route traffic through packet security gateway 910 does not indicate that the switching matrix would cause the LAN switch to drop any packets. Rather, this description of the function of the "switching matrix"—"rout[ing] network traffic"—is substantially the same as the description provided in the first paragraph— routing the packets to specified hosts—namely, "one or more of hosts A 902, B 904, and C 906" (the '077 Patent,19:2-6, 19:10-14).

1054. As I discussed above, nowhere does the '077 Patent describe or suggest that a switch matrix is modified to cause a LAN switch to drop any packets. In addition, a person of ordinary skill would not understand that the '077 Patent specification inherently discloses computer "instructions" that are executed to "modify a switching matrix of a local area

network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device." '077 Patent, Claims 7 and 13. In particular, I understand that for a feature to be inherently disclosed in the written description, it is required that such a feature necessarily be present in the description. Nothing in the '077 Patent specification would require that modifying a switching matrix would cause a LAN switch to drop any packets. For example, the "switching matrix [being] configured to switch packets received from one or more of hosts A 902, B 904, and C 906 to one or more of hosts A 902, B 904, and C 906" would require that the packets to and from these hosts not be dropped, because if any packets were dropped, they would not be routed "to one or more of hosts A 902, B 904, and C 906." '077 Patent, at 19:2-6. Likewise, the '077 Patent specification's disclosure that "packet security gateway 910 may be a device distinct from LAN switch 908, and LAN switch 908 may be configured to route network traffic through packet security gateway 910 (e.g., by modifying LAN switch 908's switching matrix)" does not require that "modifying LAN switch 908's switching matrix" would cause packets to be dropped. '077 Patent, at 19:10-14. In particular, even assuming that one of the functions performed by packet security gateway 910 is to drop packets, a person of ordinary skill in the art would understand the dropping function to be performed by the packet security gateway 910, not by the LAN switch 908 or its switching matrix. In particular, as this disclosure explains, "packet security gateway 910 may be a device distinct from LAN switch 908." '077 Patent, at 19:10-12. Accordingly, a person of skill in the art would understand that packet security gateway 910 would drop any packets that needed to be dropped and only forward those packets to LAN switch 908 that needed to be routed, such as "to one or more of hosts A 902, B 904, and C 906." '077 Patent, at 19:2-6. As such, the '077 Patent

specification does not inherently disclose computer "instructions" that are executed to "modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device." '077 Patent, Claims 7 and 13.

1055. As the '077 Patent specification provides no disclosure of computer "instructions" that are executed to "modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device," it is my opinion that Claims 7 and 13 are not disclosed in the '077 Patent specification in the manner required by 35 U.S.C. § 112, first paragraph, and therefore I believe that Claims 7 and 13 are invalid for failure to satisfy the written description requirement.

XVI. DECLARATION

1056. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that those statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: July 30, 2018



Adam Sorini, Ph.D., C.C.F.P.

APPENDIX A

Curriculum Vitae of Dr. A. Sorini

CENTRIPETAL-CSCO 087869

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 369



Exponent®
Engineering & Scientific Consulting

Adam Sorini, Ph.D., CCFP-US
Senior Managing Scientist | Electrical Engineering & Computer Science
149 Commonwealth Drive | Menlo Park, CA 94025
(650) 688-6914 tel | asorini@exponent.com

Professional Profile

Dr. Sorini is a forensics expert specializing in investigations of consumer electronics and computer technologies. Dr. Sorini's work concerns failure analysis of electronics, intellectual property matters, X-ray Computed Tomography (CT), and topics in applied computer science including diverse aspects of cybersecurity such as medical device security, network security, and digital forensics. Dr. Sorini has investigated state-of-the-art consumer electronics hardware, firmware, and software.

Dr. Sorini has a background in computational physics and numerical modelling. While at Stanford and then at Lawrence Livermore National Laboratory, Dr. Sorini implemented massively-parallel sparse-matrix computer software to determine physical properties of electronic systems. Dr. Sorini has experience with a number of computer programming languages including C, C++, FORTRAN, Python, and Java. He also has experience working with very large scale source code databases, both as a software developer and as a technical consultant.

Academic Credentials & Professional Honors

Ph.D., Physics, University of Washington, 2008

M.S., Physics, University of Washington, 2003

B.S., Physics, University of Michigan, Ann Arbor, with distinction, 2001

Licenses and Certifications

Certified Cyber Forensics Professional (CCFP), #519162

Prior Experience

Postdoctoral Researcher, Lawrence Livermore National Laboratory, 2011-2012

Postdoctoral Researcher, Stanford Institute for Materials and Energy Science, 2009-2011

Research Assistant, University of Washington, 2005-2008

Teaching Assistant, University of Washington, 2002-2005

CENTRIPETAL-CSCO 087870

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 370

Publications

Sorini A, and Staroswiecki E. Cybersecurity for the smart grid. The Power Grid: Smart, Secure, Green, and Reliable. D'Andrade B (ed). Elsevier Ltd., 2017, 233-252.

Sorini A, Jagannathan S. Self-authentication in medical device software: An approach to include cybersecurity in legacy medical devices. IEEE Symposium on Product Compliance Engineering Proceedings (ISPCE), San Jose, CA, May, 2016.

Jagannathan S, Sorini A. A cybersecurity risk assessment methodology for medical devices. Proceedings, IEEE Symposium on Product Compliance Engineering, May 2015.

Sorini A, Jagannathan S. Forensic analysis of digital time. Exponent Electrical Engineering & Computer Science Newsletter, Volume 1, 2015.

Sorini A, Jagannathan S, McGoran B. Medical device cybersecurity: Preliminary hazard analysis. Exponent Electrical Engineering & Computer Science Newsletter, Volume 1, 2015.

Sorini A, Jagannathan S. Forensic analysis of digital time. MDTC e-letter, Volume 5, No. 2, December 2014.

Huang R, Sorini A, McNulty J. Quantitative solder inspection with computer tomography. Proceedings, IEEE Symposium on Product Compliance Engineering, May 2014.

Lee JJ, Moritz B, Lee WS, Yi M, Jia CJ, Sorini AP, Kudo K, Koike Y, Zhou KJ, Monney C, Strocov V, Patthey L, Schmitt T, Devereaux TP, Shen ZX. Charge-orbital-lattice coupling effects in the dd excitation profile of one-dimensional cuprates. Physical Review B 2014; 89:041104(R).

Chuang YD, Lee WS, Kung YF, Sorini AP, Moritz B, Moore RG, Patthey L, Trigo M, Lu DH, Kirchmann PS, Yi M, Krupin O, Langner M, Zhu Y, Zhou SY, Reis DA, Huse N, Robinson JS, Kaindl RA, Schoenlein RW, Johnson SL, Forst M, Doering D, Denes P, Schlotter WF, Turner JJ, Sasagawa T, Hussain Z, Shen ZX, Devereaux, TP. Real-time manifestation of strongly coupled spin and charge order parameters in stripe-ordered nickelate crystals using time-resolved resonant X-ray diffraction. Physical Review Letters 2013; 110:127404.

Kung YF, Lee W-S, Chen C-C, Kemper AF, Sorini AP, Moritz B, Devereaux TP. Time-dependent charge-order and spin-order recovery in striped systems. Physical Review B 2013; 88:125114.

Lipp MJ, Sorini AP, Bradley J, Maddox B, Moore KT, Cynn H, Devereaux TP, Xiao Y, Chow P, Evans WJ. X-ray emission spectroscopy of cerium across the gamma-alpha volume collapse transition. Physical Review Letters 2012.;109:195705.

Lee WS, Sorini AP, Yi M, Chuang YD, Moritz B, Yang WL, Chu JH, Kuo HH, Gonzalez A, Fisher IR, Hussain Z, Devereaux TP, Shen ZX. Resonant enhancement of charge density wave diffraction in the rare-earth tritellurides. Physical Review B 2012; 85:155142.

Chuang Y-D, Moore R, Zhu Y, Patthey L, Trigo M, Lu D-H, Kirchmann P, Krupin O, Yi M, Langner M, Huse N, Robinson J, Chen Y, Zhou S, Coslovich G, Huber B, Reis D, Kaindl R, Schoenlein R, Doering D, Denes P, Schlotter W, Turner J, Johnson S, Forst M, Sasagawa T, Kung Y, Sorini A, Kemper A, Moritz B, Devereaux T, Lee D-H, Shen Z-X, Hussain Z. Phase fluctuations and the absence of topological defects in photo-excited charge ordered nickelate. Nature Communications 2012; 3:838.

Johnston S, Sorini AP, Moritz B, Devereaux TP, Scalapino DJ. Coincidence between energy gaps and Kohn anomalies in conventional super-conductors. Physical Review B 2011; 84:174523.

CENTRIPETAL-CSCO 087871

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 371

Kim YJ, Sorini AP, Stock CS, Perring TG, Van den Brink J, Devereaux TP. Probing high-energy electronic excitations using inelastic neutron scattering. Physical Review B 2011; 84:085132.

Yi M, Lu DH, Chu JH, Analytis JG, Sorini AP, Kemper AF, Mo SK, Moore RG, Hussain Z, Devereaux TP, Fisher IR, Shen Z-X. Symmetry breaking orbital anisotropy on detwinned Ba(Fe1—xCox)2As2 above the spin density wave transition. Proceedings, the National Academy of Sciences 2011; 108:6878.

Wang S, Mao WL, Sorini AP, Chen CC, Devereaux TP, Ding Y, Xiao Y, Chow P, Hiraoka N, Ishii H, Cai YQ, Kao CC. High pressure evolution of Fe2O3 electronic structure revealed by x-ray absorption. Physical Review B 2012; 82:144428.

Chen CC, Moritz B, Jia CJ, Johnston S, Sorini AP, Lee LQ, Ko K, Devereux TP. Numerical studies of photon-based spectroscopies on high-Tc superconductors. Computer Physics Communications 2010; 182:106.

Bradley JA, Seidler GT, Cooper G, Vos M, Hitchcock AP, Sorini AP, Schlimmer C, Nagle KP. Comparative study of the valence electronic excitations of N2 by inelastic x-ray and electron scattering. Physical Review Letters 2010; 105:053202.

Chen CC, Maciejko J, Sorini AP, Moritz B, Singh RRP, Devereaux TP. Orbital order and spontaneous orthorhombicity in iron pnictides. Physical Review B 2010; 82:100504(R). Editor's Choice.

Yang WL, Sorini AP, Chen CC, Moritz B, Lee WS, Vernay F, Olalde-Velasco P, Denlinger JD, Delley B, Chu JH, Analytis JG, Fisher IR, Ren ZA, Yang J, Lu W, Zhao ZX, Van den Brink J, Hussain Z, Shen Z-X, Devereaux TP. Evidence for weak electronic correlations in iron pnictides. Physical Review B 2009; 80:014508. Editor's Choice and Physics Viewpoint article.

Yang WL, Sorini AP, Chen CC, Moritz B, Lee WS, Vernay F, P. Olalde-Velasco, Denlinger JD, Delley B, Chu JH, Analytis JG, Fisher IR, Ren ZA, Yang J, Lu W, Zhao ZX, Van den Brink J, Hussain Z, Shen Z-X, DeVereaux TP. Research highlight: Evidence for weak electronic correlations in the iron pnictides. CMSN Newsletter 2009; 5:4.

Stern EA, Yacoby Y, Seidler GT, Nagle KP, Prange MP, Sorini AP, Rehr JJ, Joachimiak A. Reducing radiation damage in macromolecular crystals at synchrotron sources. Acta Crystallographica 2009; D65:366.

Rehr JJ, Kas JJ, Prange MP, Sorini AP, Takimoto Y, Vila F. Ab initio theory and calculations of x-ray spectra. C.R. Physique 2009; 10:548.

Sorini AP. The passage of fast electrons through matter. Ph.D. dissertation, University of Washington, 2008.

Sorini AP, Rehr JJ, Levine ZH. Magic angle in electron energy loss spectra: relativistic and dielectric corrections. Physical Review 2008; B 77:115126.

Sorini AP, Rehr JJ, Jorissen K. Ab initio real space calculations of electron energy loss spectra. Proceedings, AIP Conference 2008; 999:47.

Kas JJ, Sorini AP, Prange MP, Campbell LW, Soininen JA, Rehr JJ. Many pole model of inelastic losses in x-ray absorption spectra. Physical Review B 2007; 76:195116.

Rehr JJ, Kas JJ, Prange MP, Sorini AP, Campbell LW, Vila FD. Inelastic losses and multi-electron excitations in x-ray spectra. Proceedings, AIP Conference 2007; 882:85.

Sorini AP, Kas JJ, Rehr JJ, Prange MP, Levine ZH. Ab Initio calculations of mean free paths and stopping

CENTRIPETAL-CSCO 087872

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 372

powers. Physical Review B 2006; 74:165111.

Selected Speaking Engagements

Sorini A. Security-by-design for IoT devices. Arizona Technology Council Internet of Things Committee meeting, Feb 8, 2017.

Sorini A. Self-authentication in medical device software: An approach to include cybersecurity in legacy medical devices. IEEE Symposium on Product Compliance Engineering Proceedings (ISPCE), San Jose, CA, May, 2016.

Jagannathan S, Sorini A. A cybersecurity risk analysis methodology for medical devices. IEEE Symposium on Product Compliance Engineering. Chicago, IL. May 2015.

Sorini A, Huang R, McNulty J. Quantitative solder inspection with computer tomography. IEEE Symposium on Product Compliance Engineering. San Jose, CA. 2014.

Sorini A, Bradley J, Lipp M, Devereaux T. Pressure dependent x-ray emission satellites in rare-earth metals. Lawrence Livermore National Laboratory, Livermore, CA, September 2011.

Sorini A, Chen C-C, Wang S, Mao W, Devereaux T. Theoretical x-ray spectroscopy for strongly correlated materials at high pressure. APS March Meeting, Dallas, TX, March 2011.

Sorini A, Yang W, Chen C-C, Moritz B, Lee W-S, Vernay F, Olalde-Velasco P, Denlinger J, Delley B, Chu J-H, Analytis J, Fisher I, Ren Z, Yang J, Lu W, Zhao Z-X, Van den Brink J, Hussain Z, Shen Z-X, Devereaux T. Evidence for weak electronic correlations in Fe Pnictides. APS March Meeting, Portland, OR, March 2010.

Sorini A, Yang W, Chen C-C, Moritz B, Lee W-S, Vernay F, Olalde-Velasco P, Denlinger J, Delley B, Chu J-H, Analytis J, Fisher I, Ren Z, Yang J, Lu W, Zhao Z-X, Van den Brink J, Hussain Z, Shen Z-X, Devereaux T. Iron pnictides: Evidence of weak correlations. SLAC IXS Workshop, Menlo Park, CA, August 2009.

Sorini A, Rehr J, Levine Z. Magic angle in EELS: Relativistic and dielectric corrections. Lawrence Livermore National Laboratory, Livermore, CA, August 2008.

Sorini A, Rehr J, Levine Z. Magic angle in EELS: Relativistic and dielectric corrections. Geballe Laboratory for Advanced Materials, Stanford University, Stanford, CA, June 2008.

Sorini A, Rehr J, Levine Z. Magic angle in EELS: Relativistic and dielectric corrections. National Institute of Standards and Technology, Gaithersburg, MD, April 2008.

Sorini A, Rehr J, Levine Z. Effect of dielectric response on the magic angle mystery in EELS. APS March Meeting, New Orleans, LA, March 2008.

CENTRIPETAL-CSCO 087873

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 373

APPENDIX A

Curriculum Vitae of Dr. A. Sorini

CENTRIPETAL-CSCO 087874

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 374



Exponent®
Engineering & Scientific Consulting

Adam Sorini, Ph.D., CCFP-US
Senior Managing Scientist | Electrical Engineering & Computer Science
149 Commonwealth Drive | Menlo Park, CA 94025
(650) 688-6914 tel | asorini@exponent.com

Professional Profile

Dr. Sorini is a forensics expert specializing in investigations of consumer electronics and computer technologies. Dr. Sorini's work concerns failure analysis of electronics, intellectual property matters, X-ray Computed Tomography (CT), and topics in applied computer science including diverse aspects of cybersecurity such as medical device security, network security, and digital forensics. Dr. Sorini has investigated state-of-the-art consumer electronics hardware, firmware, and software.

Dr. Sorini has a background in computational physics and numerical modelling. While at Stanford and then at Lawrence Livermore National Laboratory, Dr. Sorini implemented massively-parallel sparse-matrix computer software to determine physical properties of electronic systems. Dr. Sorini has experience with a number of computer programming languages including C, C++, FORTRAN, Python, and Java. He also has experience working with very large scale source code databases, both as a software developer and as a technical consultant.

Academic Credentials & Professional Honors

Ph.D., Physics, University of Washington, 2008

M.S., Physics, University of Washington, 2003

B.S., Physics, University of Michigan, Ann Arbor, with distinction, 2001

Licenses and Certifications

Certified Cyber Forensics Professional (CCFP), #519162

Prior Experience

Postdoctoral Researcher, Lawrence Livermore National Laboratory, 2011-2012

Postdoctoral Researcher, Stanford Institute for Materials and Energy Science, 2009-2011

Research Assistant, University of Washington, 2005-2008

Teaching Assistant, University of Washington, 2002-2005

CENTRIPETAL-CSCO 087875

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 375

Publications

Sorini A, and Staroswiecki E. Cybersecurity for the smart grid. The Power Grid: Smart, Secure, Green, and Reliable. D'Andrade B (ed). Elsevier Ltd., 2017, 233-252.

Sorini A, Jagannathan S. Self-authentication in medical device software: An approach to include cybersecurity in legacy medical devices. IEEE Symposium on Product Compliance Engineering Proceedings (ISPCE), San Jose, CA, May, 2016.

Jagannathan S, Sorini A. A cybersecurity risk assessment methodology for medical devices. Proceedings, IEEE Symposium on Product Compliance Engineering, May 2015.

Sorini A, Jagannathan S. Forensic analysis of digital time. Exponent Electrical Engineering & Computer Science Newsletter, Volume 1, 2015.

Sorini A, Jagannathan S, McGoran B. Medical device cybersecurity: Preliminary hazard analysis. Exponent Electrical Engineering & Computer Science Newsletter, Volume 1, 2015.

Sorini A, Jagannathan S. Forensic analysis of digital time. MDTC e-letter, Volume 5, No. 2, December 2014.

Huang R, Sorini A, McNulty J. Quantitative solder inspection with computer tomography. Proceedings, IEEE Symposium on Product Compliance Engineering, May 2014.

Lee JJ, Moritz B, Lee WS, Yi M, Jia CJ, Sorini AP, Kudo K, Koike Y, Zhou KJ, Monney C, Strocov V, Patthey L, Schmitt T, Devereaux TP, Shen ZX. Charge-orbital-lattice coupling effects in the dd excitation profile of one-dimensional cuprates. Physical Review B 2014; 89:041104(R).

Chuang YD, Lee WS, Kung YF, Sorini AP, Moritz B, Moore RG, Patthey L, Trigo M, Lu DH, Kirchmann PS, Yi M, Krupin O, Langner M, Zhu Y, Zhou SY, Reis DA, Huse N, Robinson JS, Kaindl RA, Schoenlein RW, Johnson SL, Forst M, Doering D, Denes P, Schlotter WF, Turner JJ, Sasagawa T, Hussain Z, Shen ZX, Devereaux, TP. Real-time manifestation of strongly coupled spin and charge order parameters in stripe-ordered nickelate crystals using time-resolved resonant X-ray diffraction. Physical Review Letters 2013; 110:127404.

Kung YF, Lee W-S, Chen C-C, Kemper AF, Sorini AP, Moritz B, Devereaux TP. Time-dependent charge-order and spin-order recovery in striped systems. Physical Review B 2013; 88:125114.

Lipp MJ, Sorini AP, Bradley J, Maddox B, Moore KT, Cynn H, Devereaux TP, Xiao Y, Chow P, Evans WJ. X-ray emission spectroscopy of cerium across the gamma-alpha volume collapse transition. Physical Review Letters 2012.;109:195705.

Lee WS, Sorini AP, Yi M, Chuang YD, Moritz B, Yang WL, Chu JH, Kuo HH, Gonzalez A, Fisher IR, Hussain Z, Devereaux TP, Shen ZX. Resonant enhancement of charge density wave diffraction in the rare-earth tritellurides. Physical Review B 2012; 85:155142.

Chuang Y-D, Moore R, Zhu Y, Patthey L, Trigo M, Lu D-H, Kirchmann P, Krupin O, Yi M, Langner M, Huse N, Robinson J, Chen Y, Zhou S, Coslovich G, Huber B, Reis D, Kaindl R, Schoenlein R, Doering D, Denes P, Schlotter W, Turner J, Johnson S, Forst M, Sasagawa T, Kung Y, Sorini A, Kemper A, Moritz B, Devereaux T, Lee D-H, Shen Z-X, Hussain Z. Phase fluctuations and the absence of topological defects in photo-excited charge ordered nickelate. Nature Communications 2012; 3:838.

Johnston S, Sorini AP, Moritz B, Devereaux TP, Scalapino DJ. Coincidence between energy gaps and Kohn anomalies in conventional super-conductors. Physical Review B 2011; 84:174523.

CENTRIPETAL-CSCO 087876

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 376

Kim YJ, Sorini AP, Stock CS, Perring TG, Van den Brink J, Devereaux TP. Probing high-energy electronic excitations using inelastic neutron scattering. Physical Review B 2011; 84:085132.

Yi M, Lu DH, Chu JH, Analytis JG, Sorini AP, Kemper AF, Mo SK, Moore RG, Hussain Z, Devereaux TP, Fisher IR, Shen Z-X. Symmetry breaking orbital anisotropy on detwinned Ba(Fe1—xCox)2As2 above the spin density wave transition. Proceedings, the National Academy of Sciences 2011; 108:6878.

Wang S, Mao WL, Sorini AP, Chen CC, Devereaux TP, Ding Y, Xiao Y, Chow P, Hiraoka N, Ishii H, Cai YQ, Kao CC. High pressure evolution of Fe2O3 electronic structure revealed by x-ray absorption. Physical Review B 2012; 82:144428.

Chen CC, Moritz B, Jia CJ, Johnston S, Sorini AP, Lee LQ, Ko K, Devereux TP. Numerical studies of photon-based spectroscopies on high-Tc superconductors. Computer Physics Communications 2010; 182:106.

Bradley JA, Seidler GT, Cooper G, Vos M, Hitchcock AP, Sorini AP, Schlimmer C, Nagle KP. Comparative study of the valence electronic excitations of N2 by inelastic x-ray and electron scattering. Physical Review Letters 2010; 105:053202.

Chen CC, Maciejko J, Sorini AP, Moritz B, Singh RRP, Devereaux TP. Orbital order and spontaneous orthorhombicity in iron pnictides. Physical Review B 2010; 82:100504(R). Editor's Choice.

Yang WL, Sorini AP, Chen CC, Moritz B, Lee WS, Vernay F, Olalde-Velasco P, Denlinger JD, Delley B, Chu JH, Analytis JG, Fisher IR, Ren ZA, Yang J, Lu W, Zhao ZX, Van den Brink J, Hussain Z, Shen Z-X, Devereaux TP. Evidence for weak electronic correlations in iron pnictides. Physical Review B 2009; 80:014508. Editor's Choice and Physics Viewpoint article.

Yang WL, Sorini AP, Chen CC, Moritz B, Lee WS, Vernay F, P. Olalde-Velasco, Denlinger JD, Delley B, Chu JH, Analytis JG, Fisher IR, Ren ZA, Yang J, Lu W, Zhao ZX, Van den Brink J, Hussain Z, Shen Z-X, DeVereaux TP. Research highlight: Evidence for weak electronic correlations in the iron pnictides. CMSN Newsletter 2009; 5:4.

Stern EA, Yacoby Y, Seidler GT, Nagle KP, Prange MP, Sorini AP, Rehr JJ, Joachimiak A. Reducing radiation damage in macromolecular crystals at synchrotron sources. Acta Crystallographica 2009; D65:366.

Rehr JJ, Kas JJ, Prange MP, Sorini AP, Takimoto Y, Vila F. Ab initio theory and calculations of x-ray spectra. C.R. Physique 2009; 10:548.

Sorini AP. The passage of fast electrons through matter. Ph.D. dissertation, University of Washington, 2008.

Sorini AP, Rehr JJ, Levine ZH. Magic angle in electron energy loss spectra: relativistic and dielectric corrections. Physical Review 2008; B 77:115126.

Sorini AP, Rehr JJ, Jorissen K. Ab initio real space calculations of electron energy loss spectra. Proceedings, AIP Conference 2008; 999:47.

Kas JJ, Sorini AP, Prange MP, Campbell LW, Soininen JA, Rehr JJ. Many pole model of inelastic losses in x-ray absorption spectra. Physical Review B 2007; 76:195116.

Rehr JJ, Kas JJ, Prange MP, Sorini AP, Campbell LW, Vila FD. Inelastic losses and multi-electron excitations in x-ray spectra. Proceedings, AIP Conference 2007; 882:85.

Sorini AP, Kas JJ, Rehr JJ, Prange MP, Levine ZH. Ab Initio calculations of mean free paths and stopping

CENTRIPETAL-CSCO 087877

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 377

powers. Physical Review B 2006; 74:165111.

Selected Speaking Engagements

Sorini A. Security-by-design for IoT devices. Arizona Technology Council Internet of Things Committee meeting, Feb 8, 2017.

Sorini A. Self-authentication in medical device software: An approach to include cybersecurity in legacy medical devices. IEEE Symposium on Product Compliance Engineering Proceedings (ISPCE), San Jose, CA, May, 2016.

Jagannathan S, Sorini A. A cybersecurity risk analysis methodology for medical devices. IEEE Symposium on Product Compliance Engineering. Chicago, IL. May 2015.

Sorini A, Huang R, McNulty J. Quantitative solder inspection with computer tomography. IEEE Symposium on Product Compliance Engineering. San Jose, CA. 2014.

Sorini A, Bradley J, Lipp M, Devereaux T. Pressure dependent x-ray emission satellites in rare-earth metals. Lawrence Livermore National Laboratory, Livermore, CA, September 2011.

Sorini A, Chen C-C, Wang S, Mao W, Devereaux T. Theoretical x-ray spectroscopy for strongly correlated materials at high pressure. APS March Meeting, Dallas, TX, March 2011.

Sorini A, Yang W, Chen C-C, Moritz B, Lee W-S, Vernay F, Olalde-Velasco P, Denlinger J, Delley B, Chu J-H, Analytis J, Fisher I, Ren Z, Yang J, Lu W, Zhao Z-X, Van den Brink J, Hussain Z, Shen Z-X, Devereaux T. Evidence for weak electronic correlations in Fe Pnictides. APS March Meeting, Portland, OR, March 2010.

Sorini A, Yang W, Chen C-C, Moritz B, Lee W-S, Vernay F, Olalde-Velasco P, Denlinger J, Delley B, Chu J-H, Analytis J, Fisher I, Ren Z, Yang J, Lu W, Zhao Z-X, Van den Brink J, Hussain Z, Shen Z-X, Devereaux T. Iron pnictides: Evidence of weak correlations. SLAC IXS Workshop, Menlo Park, CA, August 2009.

Sorini A, Rehr J, Levine Z. Magic angle in EELS: Relativistic and dielectric corrections. Lawrence Livermore National Laboratory, Livermore, CA, August 2008.

Sorini A, Rehr J, Levine Z. Magic angle in EELS: Relativistic and dielectric corrections. Geballe Laboratory for Advanced Materials, Stanford University, Stanford, CA, June 2008.

Sorini A, Rehr J, Levine Z. Magic angle in EELS: Relativistic and dielectric corrections. National Institute of Standards and Technology, Gaithersburg, MD, April 2008.

Sorini A, Rehr J, Levine Z. Effect of dielectric response on the magic angle mystery in EELS. APS March Meeting, New Orleans, LA, March 2008.

CENTRIPETAL-CSCO 087878

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 378

APPENDIX B

'205 Patent Analysis

TippingPoint IPS

Contents

Claim 17 Analysis 1
Claim 33 Analysis 22

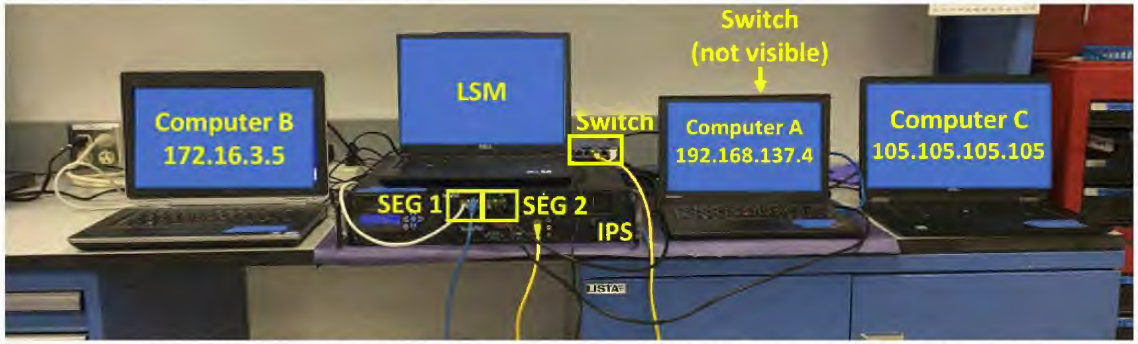
Claim 17 Analysis

Claim 17	Analysis of TippingPoint IPS
17a. A system, comprising: a security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to:	The TippingPoint UnityOne-200 Intrusion Prevention System (hereinafter, "TippingPoint IPS" or "TippingPoint system") is a system, comprising: a security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to satisfy all elements of Claim 17. Exponent obtained a TippingPoint IPS device with part number SBASY-199 Rev: C03 and serial number ST05170004, as shown in Figure 1. As required by the patent, the TippingPoint system comprises two packet security gateways (SEG 1 and SEG 2) and one security policy management server (the local security manager, or LSM), as described further below.

Claim 17	Analysis of TippingPoint IPS
	 **Figure 1: TippingPoint IPS hardware showing the part number and serial number of the device.** The TippingPoint IPS includes a local security manager (LSM), which "is the control center from which you can configure, monitor, and report on the UnityOne Intrusion Prevention System (IPS) devices in your network."[1]

[1] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. xi.

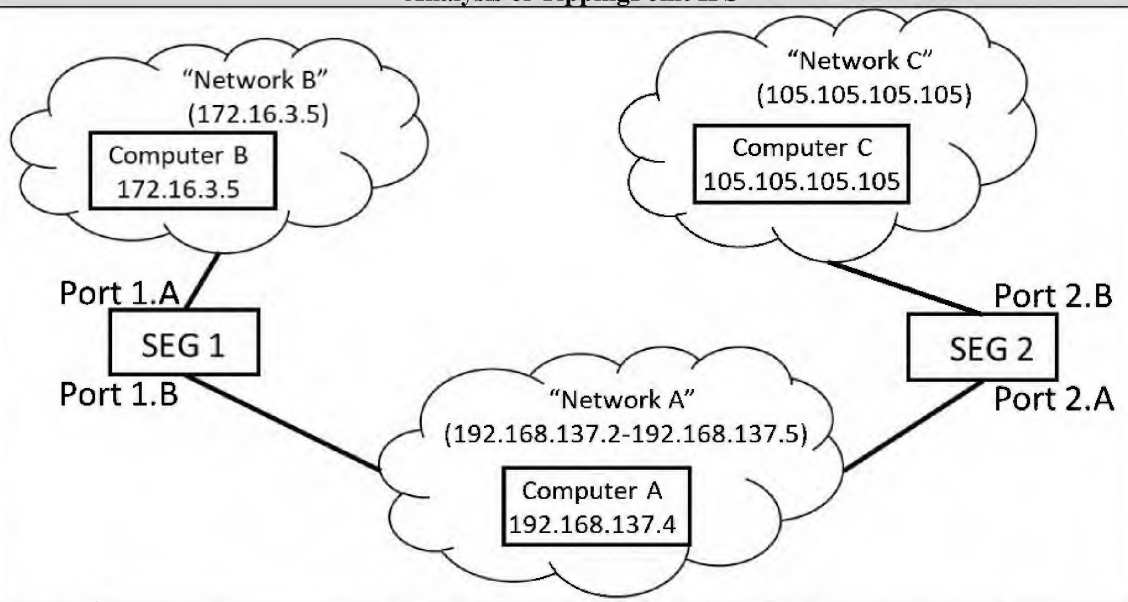
Claim 17	Analysis of TippingPoint IPS
	 **Figure 2: Annotated photographs of the TippingPoint IPS showing two packet security gateway interfaces (lower left) and one management interface (lower right).** The TippingPoint IPS also includes two separate Ethernet port pairs called "segments," which act as two separate packet security gateways; each segment can be programmed to follow its own set of filtering rules via the LSM. As such, the LSM is a security policy management server which can provide rules, messages, instructions, etc. to the segment packet security gateways. Additional security policy management server functionality is performed in part via a web server running on the MGMT Ethernet interface of the TippingPoint IPS, indicated in the red annotations in Figure 2.

Claim 17	Analysis of TippingPoint IPS
	The TippingPoint IPS LSM "is a graphical user interface (GUI) that enables you to monitor and configure your UnityOne Intrusion Prevention System (IPS) using an ordinary web browser."[2] To access this GUI, an Ethernet cable was connected between the MGMT port of the IPS and a computer running Windows XP with Internet Explorer 7.[3] An image of the system is shown in Figure 3:  **Figure 3: Image of test network used as part of the claim analysis that shows a hardware installation of one IPS containing a security management server and two packet security gateways ("SEG 1" and "SEG 2"). The laptop labeled "LSM" is used to connect to the LSM located on the TippingPoint IPS device. Computers A, B, and C reside in separate network address spaces and are connected by the two packet security gateways.** Figure 3 shows the physical layout of the hardware, including the IPS with its two packet security gateways (SEG 1 and SEG 2) and the security management server (located on-board the Tipping Point IPS device), the LSM interface laptop, two switches, and three additional laptop computers for sending and receiving packet traffic. The test network shown in Figure 3 includes computers with IP addresses in three different network

[2] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 8.

[3] The TippingPoint IPS web server was found to be incompatible with modern versions of Internet Explorer. Internet Explorer 7 was released circa 2006. (See, for example, https://en.wikipedia.org/wiki/Internet_Explorer_version_history#Windows_Internet_Explorer_7.)

Claim 17	Analysis of TippingPoint IPS
	address spaces. Only two these computers (and only one TippingPoint IPS) segment are used to illustrate how the TippingPoint system performs the method of Claims 17 and 33. The second segment was initially used to illustrate how the TippingPoint system performed the method of Claims 91, 93, and 95 of the '205 patent, which were a part of the original matter but have since been removed. The first network is called "Network A" and includes IP addresses in the range from 192.168.1.37.2 through 192.168.137.5. Network traffic internal to Network A is communicated via a TP-Link TL-SG108 Switch (not visible in Figure 3). The second network is called "Network B" and includes a computer with IP address 172.16.3.5. Network A and Network B are used to illustrate how the TippingPoint system performs the method of Claim 17. Network A and Network B are connected by the first packet security gateway, which is the packet security gateway labeled SEG 1 in Figure 3. The test network shown in Figure 3 also includes a third network, called "Network C," that includes a computer with IP address 105.105.105.105. Network A and Network C are connected by the second packet security gateway, which is the packet security gateway labeled SEG 2 in Figure 3. Only one packet security gateway is used to illustrate how the TippingPoint system performs the method of Claim 17 and 33. Both packet security gateways were used to illustrate how the TippingPoint system performs the method of Claims 91, 93, and 95 of the '205 patent, which were a part of the original matter but have since been removed. Figure 4 shows the schematic layout of the networks. Network A includes Computer A. Network B includes Computer B. Network C includes Computer C. The first packet security gateway (SG1, associated with Segment 1, or SEG 1) protects Network B from Network A. The second packet security gateway (SG2, associated with Segment 2, or SEG 2) protects Network C from Network A.

Claim 17	Analysis of TippingPoint IPS
	 **Figure 4: Schematic of the test network (see Figure 3) architecture, including the static IP addresses of each element. Each network has its own subnet. SEG 1 protects Network B from Network A. SEG 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (Port A and Port B), which are used to pass traffic between networks.**
17b. receive a plurality of dynamic security policies from the security policy management server;	As configured in Figure 4, the security gateway SEG 1 receives a plurality of dynamic security policies from the security policy management server. A dynamic security policy "includes any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to that [sic] criteria."[4] Figure 5 shows some of the 1,888 filters that are available by default on the TippingPoint IPS. These

[4] '205 Patent, Column 4, Lines 43–47.

Claim 17	Analysis of TippingPoint IPS
	filters can be adjusted to perform various user-defined transformation functions (such as allowing, blocking, logging, and/or copying) on packets corresponding to the relevant criteria.

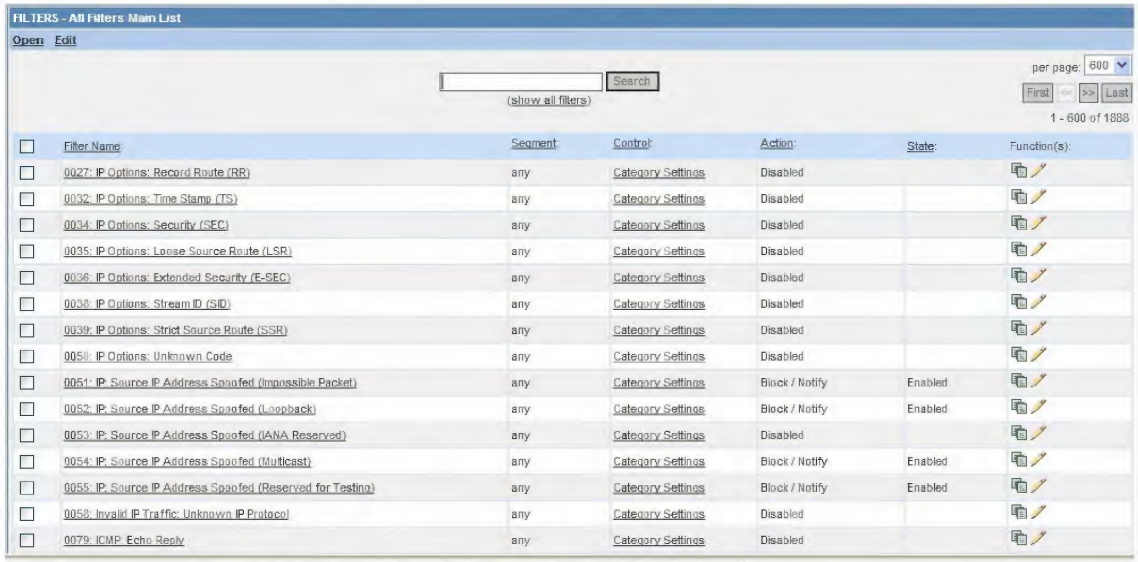


Figure 5: Sample filters available in the IPS.

Each of these independent filters can be set to a series of actions that either block or permit the packet. An example filter is shown in Figure 6—filter 0361: "HTTP Protected File Access (/etc/passwd)." The "save" button in the lower right corner updates the filter settings.

Claim 17	Analysis of TippingPoint IPS

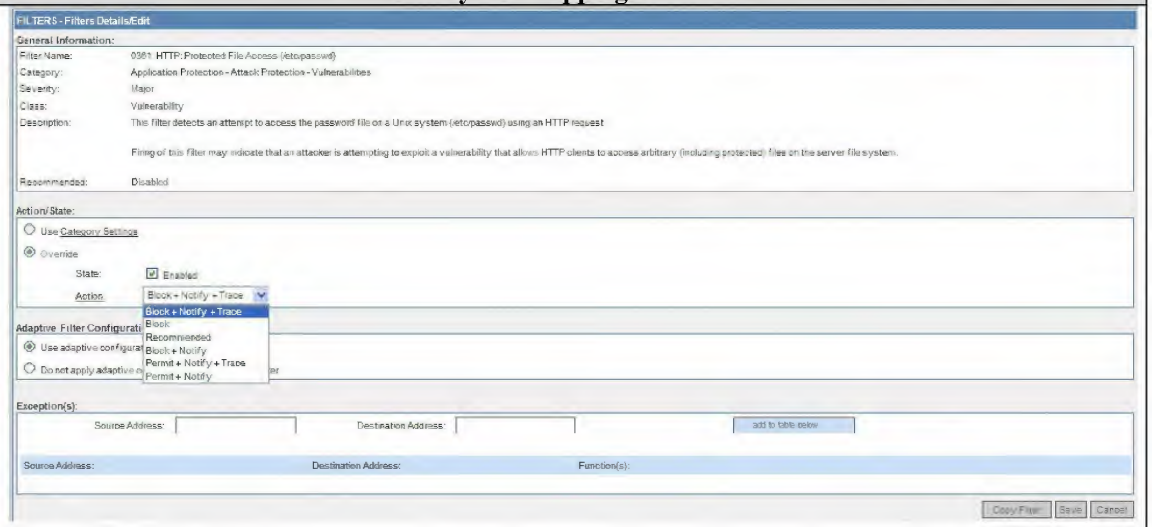


Figure 6: Filter 0361, which "detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request." A series of actions are possible for packets that are identified by this filter.

Blocked packets are intercepted and logged in a Block Log, as is shown in Figure 7.

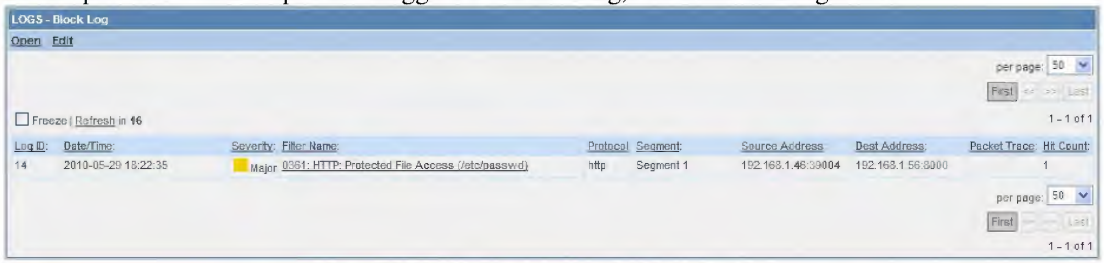


Figure 7: Block Log, which shows the blocked packets.

Permitted packets are logged in an Alert Log while the packets are allowed to continue to their destination.

CENTRIPETAL-CSCO 087888

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 388

Claim 17	Analysis of TippingPoint IPS

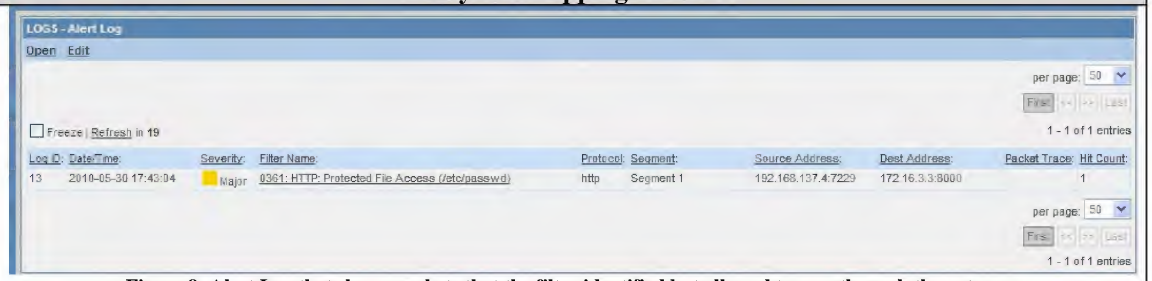


Figure 8: Alert Log that shows packets that the filter identified but allowed to pass through the gateway.

In addition to the filters listed above, user-defined traffic management filters can filter packets based on source and destination IP addresses. Figure 9 shows a sample of the traffic management filters screen with eight filters entered.

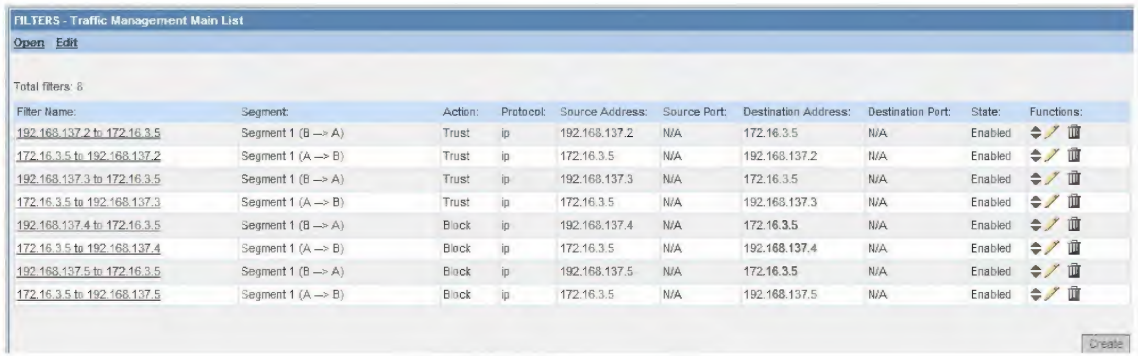
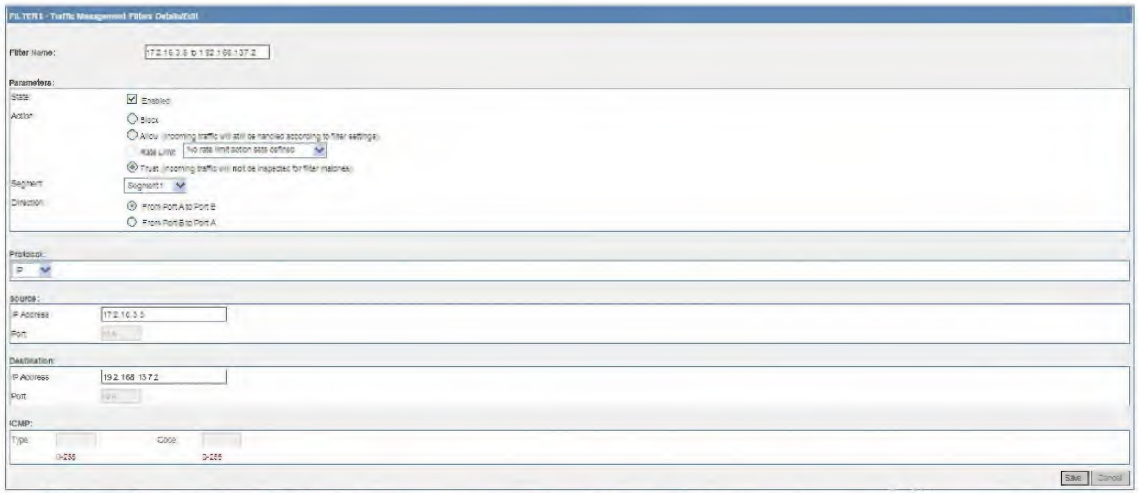


Figure 9: Traffic management filters.

Each traffic management filter can be customized through various parameters. A screenshot displaying these parameters are shown in Figure 10; the "save" button in the lower right corner creates/updates the filter. Note that the "Allow" setting means that the packets will still be inspected against the other

Claim 17	Analysis of TippingPoint IPS
	dynamic security policies within the system, while the "Trust" setting means that the packets will not be inspected against the other dynamic security policies within the system.[5]  **Figure 10: Parameters for defining a traffic management filter. The "save" button in the lower right corner creates the filter.** Thus, the security gateways can receive dynamic security policies from the security policy management server. This process is illustrated in more detail below.
17c. receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the	As configured in Figure 4, the security gateway SEG 1 receives at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped. The TippingPoint system was configured with an initial security policy consisting of eight explicit rules. The first two explicit rules allow any traffic between IP addresses 192.168.137.2 and 172.16.3.5 to

[5] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 89.

Claim 17	Analysis of TippingPoint IPS
set of network addresses for which packets should be forwarded should be dropped;	transmit, and the second two explicit rules allow any traffic between IP addresses 192.168.137.3 and 172.16.3.5. Rules 5 and 6 block traffic between IP addresses 192.168.137.4 and 172.16.3.5, and Rules 7 and 8 block traffic between IP addresses 192.168.137.5 and 172.16.3.5. The computers we used in this test have IP addresses 192.168.137.4 and 172.16.3.5, which means that traffic between these two test computers should be blocked for this initial rule set. Figure 11 is a screenshot from the LSM GUI showing this security policy configuration.

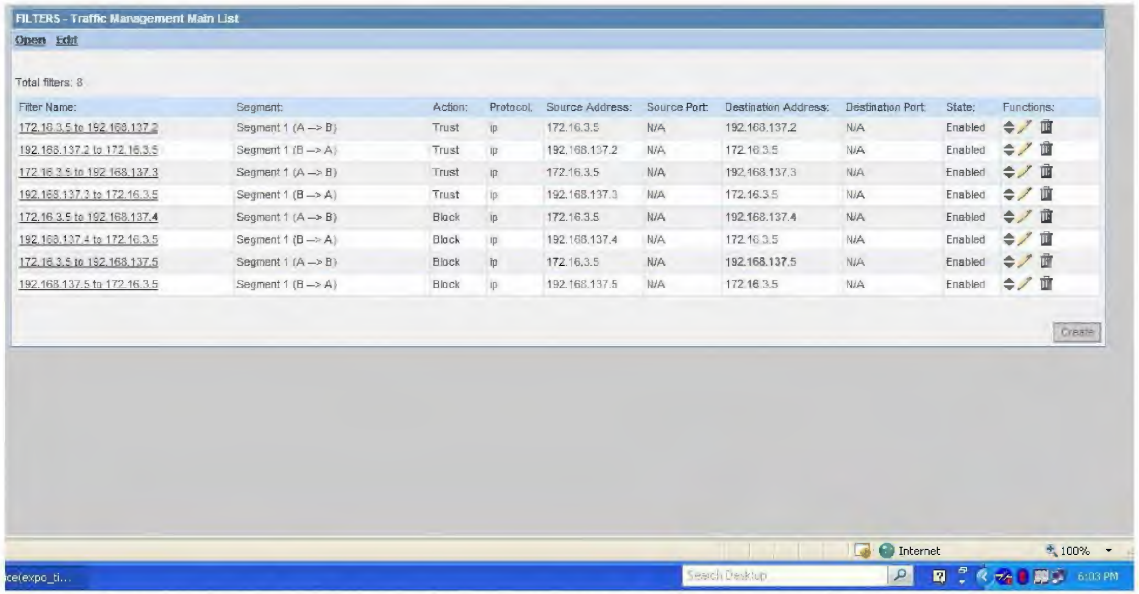


Figure 11: Screenshot of The LSM GUI showing the first dynamic security policy with eight explicit rules. The top four rules allow packet transmission, and the bottom four rules block packet transmission.

The policies were installed on Segment 1, as the screenshot in Figure 11 shows. Each row for the State column displays "Enabled," meaning that the policy is currently in effect.

To demonstrate the operation of the security policy, Exponent first attempted to ping Computer A from

Claim 17	Analysis of TippingPoint IPS
	Computer B through security gateway 1 (see Figure 12). By default, the command line transmitted four ping requests, all of which failed to receive a reply from Computer A.

```
C:\Users\Tester>time /t
06:03 PM

C:\Users\Tester>ping 192.168.137.4

Pinging 192.168.137.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.137.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Tester>time /t
06:03 PM
```

Figure 12: Attempt to ping Computer A from Computer B.

Exponent then attempted to ping Computer B from Computer A (see Figure 13), which likewise failed to show a reply:

```
C:\Users\nhorton>time /t
06:03 PM

C:\Users\nhorton>ping 172.16.3.5

Pinging 172.16.3.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

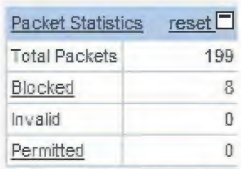
Ping statistics for 172.16.3.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

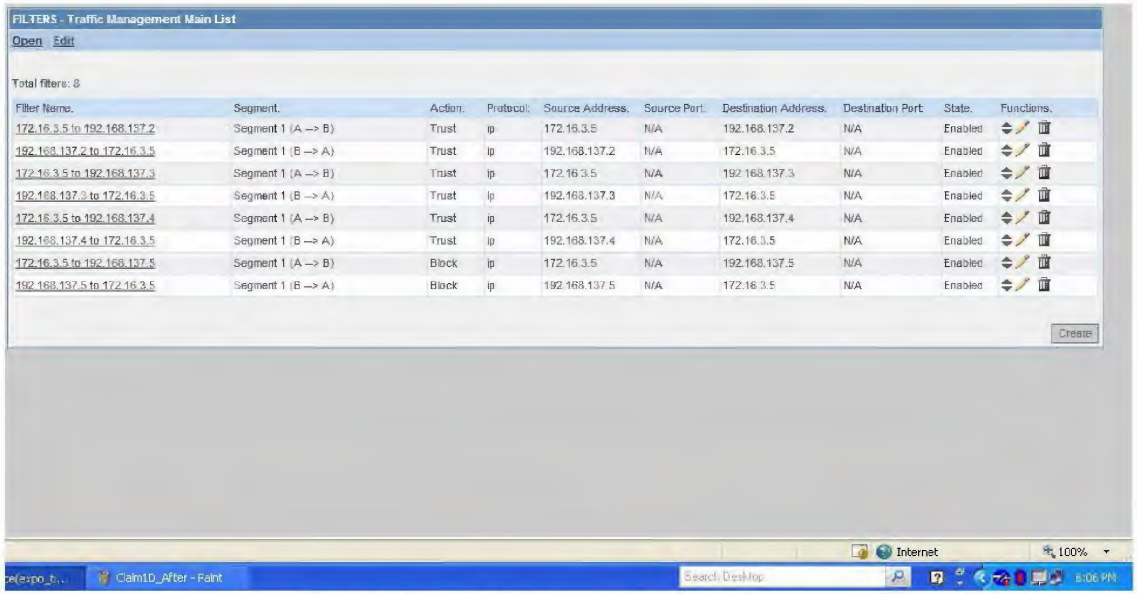
C:\Users\nhorton>time /t
06:03 PM
```

Figure 13: Attempt to ping Computer B from Computer A.

CENTRIPETAL-CSCO 087892

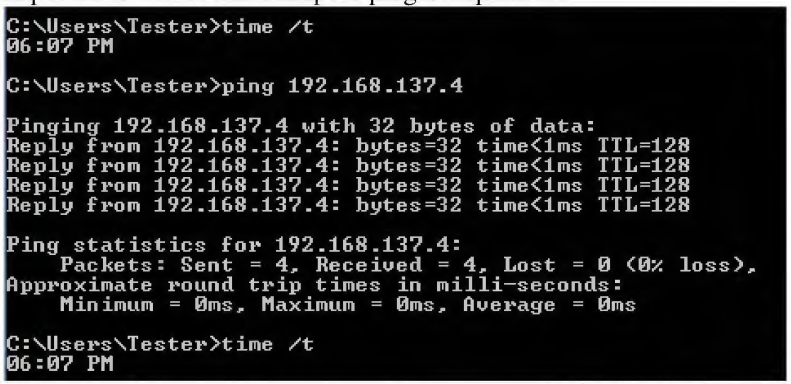
Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 392

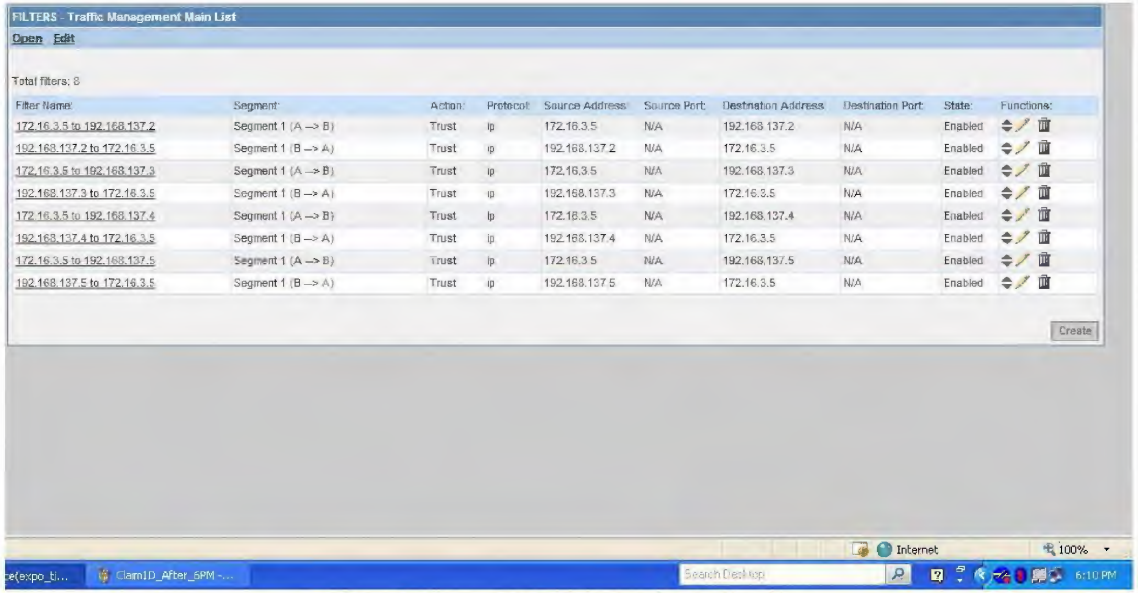
Claim 17	Analysis of TippingPoint IPS
	The LSM GUI contains a "Packet Statistics" panel that displays the number of blocked packets. The number, which was reset to 0 before this testing began, rose to eight after the four ping requests were sent from each computer, which is additional evidence that all eight ping packets were blocked by the security gateway.  **Figure 14: The eight blocked packets comprise the four ping requests from Computer A to Computer B, and the four ping requests from Computer B to Computer A.** Thus, it has been demonstrated that this security policy includes at least one rule specifying a set of network addresses for which associated packets should be forwarded (Rules 1–4) and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped (Rules 5–8).
17d. receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	As configured in Figure 4, the security gateway SEG 1 receives, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded. At 6:03 pm, as recorded by the clock on the computer running the LSM, Segment 1 received the dynamic security policy outlined in the analysis of claim element 17c (see the desktop clock located in the lower right corner of Figure 11). These policies specified that traffic should be forwarded for hosts with IP addresses in the range 192.168.137.2–192.168.137.3. This behavior is demonstrated in the analysis of claim element 17c, where it was shown that a host with an address outside this first set of network addresses is blocked. Thus, it has been demonstrated that a dynamic security policy specifying a set of network addresses for which packets should be forwarded was received by the TippingPoint IPS at a first time.

Claim 17	Analysis of TippingPoint IPS
17e. receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	TippingPoint IPS is a system that receives, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded. As shown in Figure 15, at 6:06 pm (as recorded by the clock on the computer running the LSM) security gateway Segment 1 received a security policy with a second set of network addresses for which packets should be forwarded, contained in Lines 5 and 6. This range includes more network addresses than the range in the security policy in claim element 17d. The time at which this second security policy was installed was later than the time at which the first security policy was installed.  FILTERS - Traffic Management Main List Open Edit Total filters: 8 Filter Name. Segment. Action. Protocol. Source Address. Source Port. Destination Address. Destination Port. State. Functions. 172.16.3.5 to 192.168.137.2 Segment 1 (A --> B) Trust ip 172.16.3.5 N/A 192.168.137.2 N/A Enabled 192.168.137.2 to 172.16.3.5 Segment 1 (B --> A) Trust ip 192.168.137.2 N/A 172.16.3.5 N/A Enabled 172.16.3.5 to 192.168.137.3 Segment 1 (A --> B) Trust ip 172.16.3.5 N/A 192.168.137.3 N/A Enabled 192.168.137.3 to 172.16.3.5 Segment 1 (B --> A) Trust ip 192.168.137.3 N/A 172.16.3.5 N/A Enabled 172.16.3.5 to 192.168.137.4 Segment 1 (A --> B) Trust ip 172.16.3.5 N/A 192.168.137.4 N/A Enabled 192.168.137.4 to 172.16.3.5 Segment 1 (B --> A) Trust ip 192.168.137.4 N/A 172.16.3.5 N/A Enabled 172.16.3.5 to 192.168.137.5 Segment 1 (A --> B) Block ip 172.16.3.5 N/A 192.168.137.5 N/A Enabled 192.168.137.5 to 172.16.3.5 Segment 1 (B --> A) Block ip 192.168.137.5 N/A 172.16.3.5 N/A Enabled Create Internet 100% Claim1D_After - Paint 6:06 PM **Figure 15: Screenshot of the second dynamic security policy.** The range of network addresses that should be forwarded according to Rule 2 in this second security policy includes the address of Computer A.

CENTRIPETAL-CSCO 087894

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 394

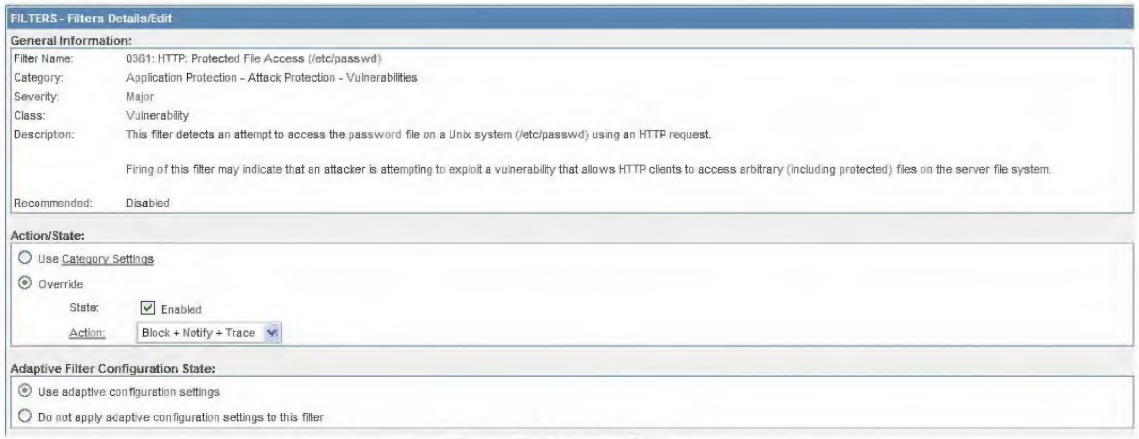
Claim 17	Analysis of TippingPoint IPS
	To demonstrate the operation of the second set of dynamic security policies, Exponent attempted to send packets from Computer A to Computer B according to Rule 2, which should be allowed by this rule set. First, Exponent attempted to ping Computer B from Computer A (see Figure 16). These ping requests were allowed to transmit indicating that Segment 1 was forwarding packets from Computer B to Computer A as well as Computer A to Computer B, as required by Rules 5 and 6. Figure 16 is a screenshot of Computer B's successful attempt to ping Computer A.  **Figure 16: Screenshot of ping from Computer A ("exponent-laptop") to Computer B (172.16.1.99) indicating 0% packet loss, demonstrating that the security gateway forwarded the packets.** Thus, it has been demonstrated that a dynamic security policy specifying a set of network addresses for which packets should be forwarded was received. Based on Exponent's analysis of network traffic and the TippingPoint documentation, the rules of this security policy allow packets to be forwarded through the security gateway (SG1).
17f. receive, at a third time, a dynamic security policy specifying a third set of network addresses for which	As configured in Figure 4, the security gateway SEG 1 receives, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network

Claim 17	Analysis of TippingPoint IPS
packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;	addresses including more network addresses than the second set of network addresses. As shown in Figure 17, at 6:10 pm (as recorded by the clock on the computer running the LSM), SG1 received a security policy with a third set of network addresses for which packets should be forwarded. This range includes more network addresses than the range in the security policy in claim element 17e.  FILTERS - Traffic Management Main List Open Edit Total filters: 8 Filter Name: Segment: Action: Protocol: Source Address: Source Port: Destination Address: Destination Port: State: Functions: 172.16.3.5 to 192.168.137.2 Segment 1 (A --> B) Trust ip 172.16.3.5 N/A 192.168.137.2 N/A Enabled 192.168.137.2 to 172.16.3.5 Segment 1 (B --> A) Trust ip 192.168.137.2 N/A 172.16.3.5 N/A Enabled 172.16.3.5 to 192.168.137.3 Segment 1 (A --> B) Trust ip 172.16.3.5 N/A 192.168.137.3 N/A Enabled 192.168.137.3 to 172.16.3.5 Segment 1 (B --> A) Trust ip 192.168.137.3 N/A 172.16.3.5 N/A Enabled 172.16.3.5 to 192.168.137.4 Segment 1 (A --> B) Trust ip 172.16.3.5 N/A 192.168.137.4 N/A Enabled 192.168.137.4 to 172.16.3.5 Segment 1 (B --> A) Trust ip 192.168.137.4 N/A 172.16.3.5 N/A Enabled 172.16.3.5 to 192.168.137.5 Segment 1 (A --> B) Trust ip 172.16.3.5 N/A 192.168.137.5 N/A Enabled 192.168.137.5 to 172.16.3.5 Segment 1 (B --> A) Trust ip 192.168.137.5 N/A 172.16.3.5 N/A Enabled Create Internet 100% Claim1D_After_5PM -... Search Desktop 6:10 PM **Figure 17: Screenshot of third dynamic security policy.** The testing described in claim elements 17d-17f demonstrated that the security gateway received three dynamic security policies. The first policy allowed transmission of packets from IP address in the range of 192.168.137.2–192.168.137.3, the second policy forwarded packets in the range of 192.168.137.2–192.168.137.4, and the third policy allowed transmission of packets in the range of 192.168.137.2–192.168.137.5. As recorded by the clock on the computer running the LSM, the first policy was received

Claim 17	Analysis of TippingPoint IPS
	at 6:03 pm, the second policy was received at 6:06 pm, and the third policy was received at 6:10 pm. Thus, it has been demonstrated that the second policy was received after the first policy, and the third policy was received after the second policy. Exponent has also demonstrated that the second set of network addresses included more network addresses than the first set, and the third set of network addresses included more network addresses than the second set.
17g. receive packets associated with a network protected by the packet security gateway;	As configured in Figure 4, the security gateway SEG 1 receives packets associated with a network protected by the packet security gateway. As was shown in claim element 17e, Computer B was successfully able to ping Computer A using Internet Control Message Protocol (ICMP) packets. Thus, it has been demonstrated that the TippingPoint IPS method includes receiving packets associated with a network protected by the packet security gateway.
17h. and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the	The TippingPoint IPS is a system that performs, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets. As stated in the patent, routing a packet to a monitoring device is an example of a packet transformation function other than forwarding or dropping.[6] The TippingPoint system has the ability to log information about network traffic.[7] For packets that are identified by filters in the LSM, matching events can be tracked. The gateways collect log data, which are available for review via the LSM. The LSM server makes logs and tracked packets available for inspection via the LSM GUI.

[6] '205 Patent, Column 7, Lines 27–36.

[7] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at Section 4.

Claim 17	Analysis of TippingPoint IPS
plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.	This logging function is a packet transformation function other than forwarding or dropping packets. One security policy used during the testing was configured to block packet traffic involved in making an HTTP request for the sensitive file path "/etc/passwd." For this testing, Computer A hosted an HTTP server and Computer B attempted to access the "/etc/passwd" file via an HTTP GET request. The filter settings are shown in Figure 18.  **Figure 18: /etc/passwd filter.** All eight security rules (described in the previous analysis) that were previously configured to "Trust" were altered to "Allow" (see Figure 19).[8] This means that the IP ranges will be allowed to communicate. However, the traffic will now be inspected by the TippingPoint system and may be blocked due to IPS rules such as the one shown in Figure 18.

[8] The ordering of the rules is slightly different (A→B and B→A Segment rule positions are swapped) than in the figures shown in the analysis of claim elements 17d, 17e, and 17f. However, the meaning of the rules is the same.

Claim 17	Analysis of TippingPoint IPS

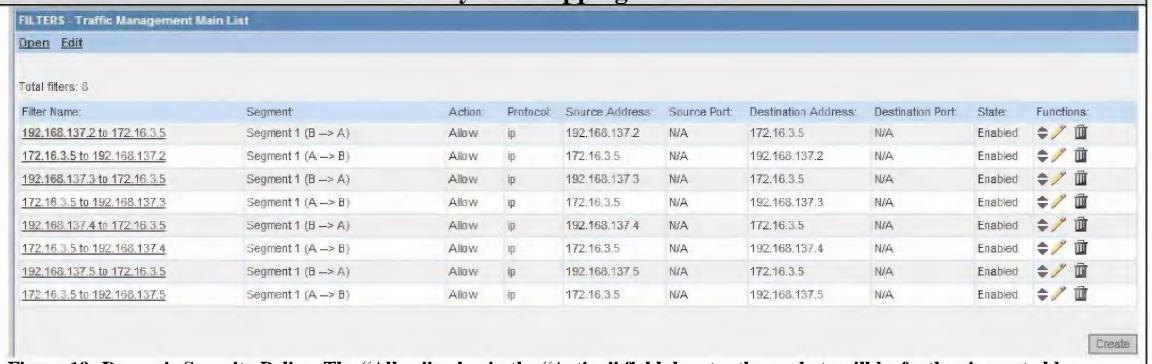


Figure 19: Dynamic Security Policy. The "Allow" value in the "Action" field denotes the packets will be further inspected by the IPS.

While logging was occurring, "ncat" was used to open a connection between Computer A and Computer B. An HTTP server was started on port 8000 of Computer B and was used to attempt to access the /etc/passwd file on Computer A (see Figure 20 and Figure 21).

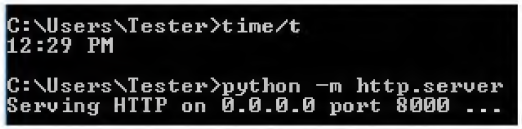


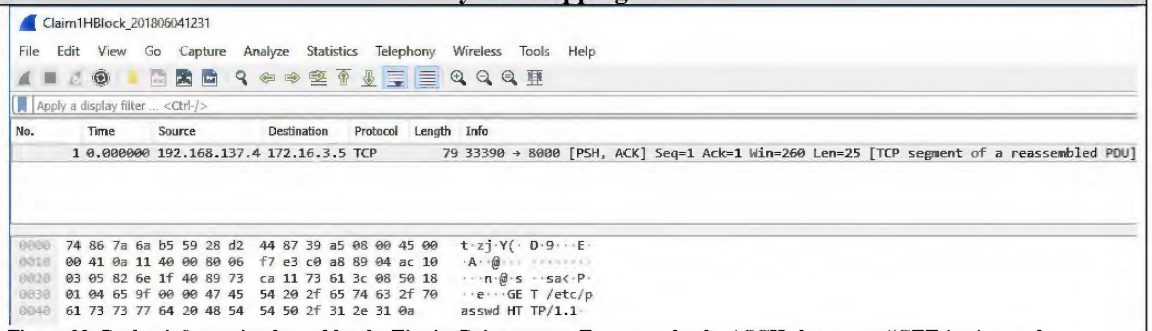
Figure 20: Hosting the HTTP website on Computer B.



Figure 21: Sending "GET /etc/passwd" request from Computer A (192.168.137.4) to Computer B (172.16.3.5) on port 8000.

Claim 17	Analysis of TippingPoint IPS
	While the current security policy was installed on Segment 1, logs were stored on the TippingPoint system and accessed by clicking the Blocked Packets button of the LSM GUI. The packet corresponding to the HTTP protected file access network threat was recorded as captured by the Block Log (see Figure 22).  **Figure 22: Screenshot from the LSM GUI showing the Block Log, which lists packets that were not forwarded to their intended destination.** By downloading the packet trace (see "Packet Trace" column in Figure 22) and opening it in Wireshark,[9] contents of the packet could be viewed (see Figure 23).

[9] Wireshark is a network analysis computer program. See, for example, https://www.wireshark.org.

Claim 17	Analysis of TippingPoint IPS
	 **Figure 23: Packet information logged by the TippingPoint system. For example, the ASCII characters "GET /etc/passwd HTTP/1.1" can be seen in the lower right section of this figure.** The TippingPoint IPS also includes monitoring, which, similar to logging, applies packet transformation functions other than forwarding or dropping. Thus, it has been demonstrated that the TippingPoint system includes logging, which is a packet transformation function other than forwarding or dropping.

Claim 33 Analysis

Claim 33	Analysis of TippingPoint IPS
33a. One or more non-transitory computer readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:	The tested TippingPoint IPS installation has one or more non-transitory computer readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to execute claim elements 33b, 33c, 33d, 33e, 33f, 33g, and 33h. As discussed in the analysis of Claim 17, the tested TippingPoint IPS installation comprises two sets of ports (labeled Segment 1 and Segment 2) functioning as packet security gateways that are both associated with a security policy management server. UnityOne-200 contains a hard drive, which is a non-transitory computer-readable medium. This hard drive has instructions stored on it that, when executed, cause each packet security gateway to perform the functionality specified in Claim 33.
33b. receive a plurality of dynamic security policies from the security policy management server;	The tested TippingPoint IPS installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive a plurality of dynamic security policies from the security policy management server. See claim element 17b.
33c. receive at least one rule specifying a set of network addresses for which associated packets should be for warded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;	The tested TippingPoint IPS installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped. See claim element 17c.

Claim 33	Analysis of TippingPoint IPS
33d. receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	The tested TippingPoint IPS installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded. See claim element 17d.
33e. receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	The tested TippingPoint IPS installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded. See claim element 17e.
33f. receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network	The tested TippingPoint IPS installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses. See claim element 17f.

Claim 33	Analysis of TippingPoint IPS
addresses;	
33g. receive packets associated with a network protected by the packet security gateway;	The tested TippingPoint IPS installation has media of claim element 33a, having instructions stored thereon, that, when executed, cause each packet security gateway to receive packets associated with a network protected by the packet security gateway. See claim element 17g.
33h. and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.	The tested TippingPoint IPS installation has media of claim element 33a, having instructions stored thereon, that, when executed, cause each packet security gateway to perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets. See claim element 17h.

APPENDIX C

'205 Patent Analysis

Check Point R75

Contents

Claim 17 Analysis 1
Claim 17 Analysis ..... **Error! Bookmark not defined.**
Claim 33 Analysis 26

Claim 17 Analysis

Claim 17	Analysis of Check Point R75
17a. A system, comprising: a security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to:	The Check Point R75 is commercial software product comprising a security management server (SMS) program,[1] which when installed on suitable hardware constitutes a security policy management server, and a security gateway (SG) program,[2] which when installed on suitable hardware constitutes of a packet security gateway. An illustration of how the Check Point R75 SG and R75 SMS fit into a typical network architecture is shown in Figure 1. Exponent assembled and tested a network configured in this arrangement,wherein the components labeled "SMS", "SG 1", and "SG 2" in Figure 2 collectively form "the Check Point R75 system." This system comprises a security policy management server and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to satisfy all elements of Claim 17.

[1] See "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010).
[2] See "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

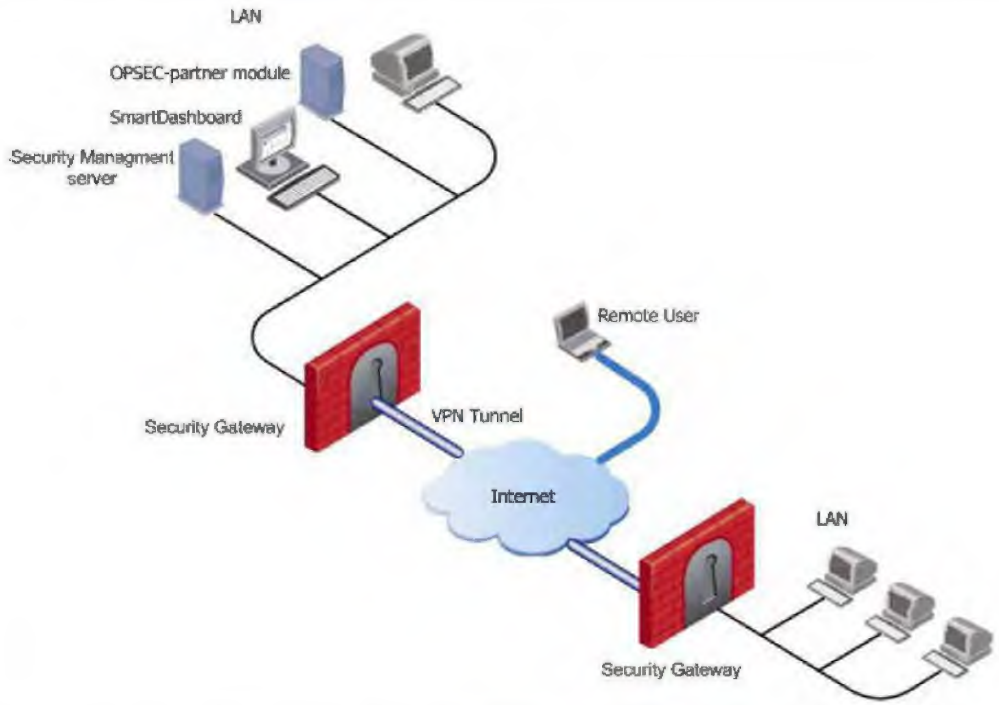


Figure 1: Illustration of a typical deployment consisting of two security gateways and a security management server (configurable using the "SmartDashboard" GUI).[3]

Exponent installed the Check Point R75 SMS product on a 32-bit PC-compatible Dell Latitude E6400 computer using the "Check_Point_R75.Splat.iso" DVD ISO image (see "SMS" in Figure 2).[4]

[3] See p. 10, "R75 Installation and Upgrade Guide" (dated Dec 15, 2010).

[4] According to the Check Point website, DVD installation material was available in December 2010 (see https://supportcenter.CheckPoint.com/supportcenter/) and the installation procedure for the Firewall and Security Management Server is documented in the "R75 Installation and Upgrade Guide."

The Check Point R75 SG product was also installed on two 32-bit PC-compatible Dell PowerEdge 1750 computers (see "SG 1" and "SG 2" in Figure 2).

The SMS and SGs were installed in a "Distributed Deployment" configuration (see Figure 1) where the SMS is installed on a different machine than the SGs.

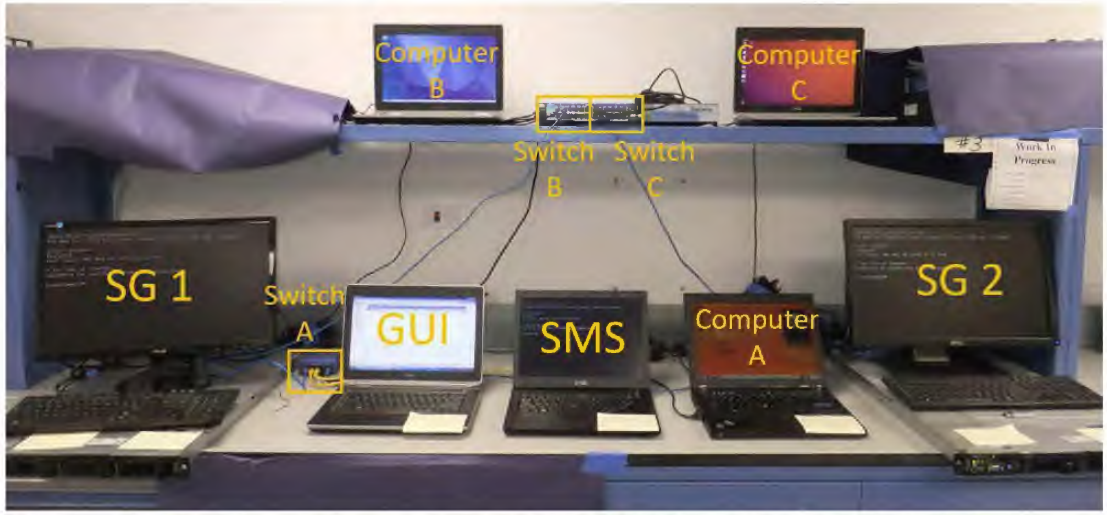
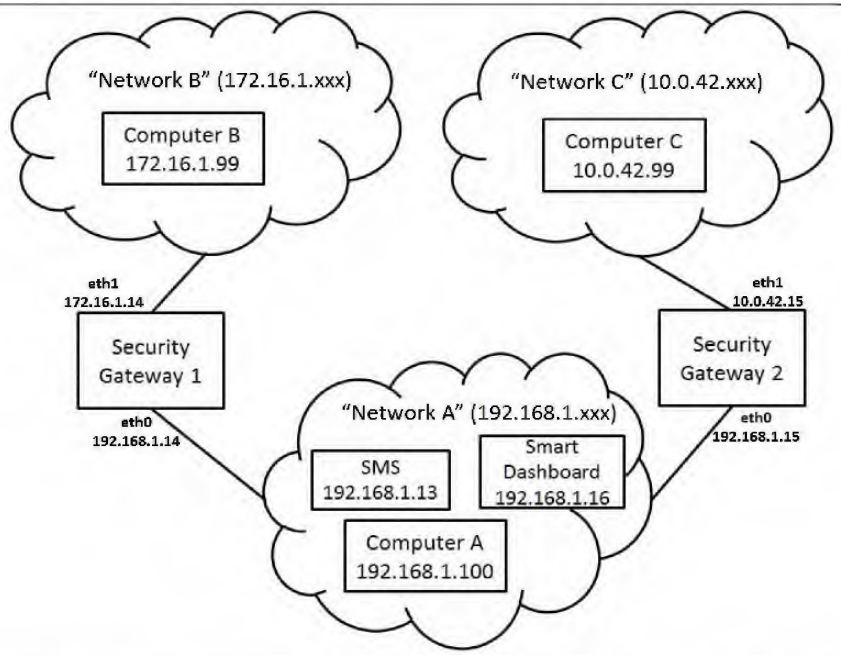


Figure 2: Photograph of test network used as part of the claim analysis that shows a hardware installation of two security gateways (SG 1 and SG 2), one security management server (SMS) with its associated SmartDashboard graphical user interface (GUI). Computers A, B, and C reside in three separate networks connected by the security gateways. Each network has one switch to route traffic.

Figure 2 shows the physical layout of the hardware, including the two security gateways, the security management server, the SmartDashboard interface, three switches, and three computers for sending and receiving traffic.

The test network shown in Figure 2 includes three subnetworks (subnets). Only two of these subnets are used to illustrate how the Check Point R75 system performs the method of Claim 17.

	The first subnet is called "Network A" and includes IP addresses in the range from 192.168.1.0 through 192.168.1.255. Network traffic internal to Network A is communicated via a TRENDent TE100-S5 switch (Switch A). The second subnet is called "Network B" and includes IP addresses in the range from 172.16.1.0 through 172.16.1.255. Network traffic internal to Network B is communicated via a VLAN on a HP ProCurve 2510-24 that uses the ProCurve Ethernet ports numbered 1—12 (Switch B). Network A and Network B are used to illustrate how the Check Point R75 system performs the method of Claim 17. Network A and Network B are connected by a R75 SG (packet security gateway), which we refer to as "Security Gateway 1" or "SG 1." This packet security gateway is also referred to as "cpgateway1" in the SmartDashboard GUI. The test network shown in Figure 2 also includes a third subnet called "Network C" that includes IP addresses in the range from 10.0.42.0 through 10.0.42.255. Network traffic internal to Network C is communicated via a VLAN on a HP ProCurve 2510-24 that uses the ProCurve Ethernet ports numbered 13–24 (Switch C). Network A and Network C are connected by a R75 SG (packet security gateway) called "Security Gateway 2" or "SG 2." This packet security gateway is also referred to as "cpgateway2" in the SmaryDashboard GUI. However, only Security Gateway 1 is necessary to illustrate how the R75 system performs the method of Claim 17; Security Gateway 2 was originally used to illustrate how the R75 system performs the method of Claims 91, 93, and 95 of the '205 patent, which were a part of the original matter but have since been removed. Figure 3 shows the schematic layout of the networks. Network A includes the R75 SMS (the security policy management server) along with another computer called "Computer A." Network B includes another computer called "Computer B." Network C includes another computer called "Computer C." Security Gateway 1 (a packet security gateway) protects Network B from Network A. Security Gateway 2 (a packet security gateway) protects Network C from Network A.

	 **Figure 3: Schematic of test network (see Figure 2) architecture, including the static IP addresses of each element. Each network has its own subnet. SG 1 protects Network B from Network A. SG 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (eth0 and eth1), which are used to pass traffic between networks.**
17b. receive a plurality of dynamic security policies from the security policy management server;	As configured in Figure 3, the security gateway SG 1 receives a plurality of dynamic security policies from the security policy management server (SMS). The patent states that "a dynamic security policy includes any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to that criteria."[5]

[5] '205 Patent, Column 4, Lines 43–47.

	According to the Check Point R75 documentation, "A Security Policy consists of an ordered set of rules, collectively known as the Rule Base. [...] The Security Gateway inspects packets and applies rules in a sequential manner. When a Security Gateway receives a packet from a connection, it inspects the packet and applies the first rule in the Rule Base, then the second rule and so on. Once all elements in a given rule match the information contained the packet (source, destination, service, etc.), the Security Gateway stops the inspection and immediately applies that rule. If no applicable rule is found in the Rule Base, the traffic is automatically blocked."[6] Thus, Check Point Security Policies are dynamic security policies. According to the Check Point R75 documentation, these security policies can be installed on selected security gateways using the security management server.[7] Thus, the security gateways can receive dynamic security policies from the security policy management server. This process is illustrated in the testing presented below.
17c. receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;	As configured in Figure 3, the security gateway SG 1 receives at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped. A security policy with two explicit rules was developed and implemented on the Check Point R75 system. The first explicit rule allows any traffic from Computer B to be forwarded. The second explicit rule allows any traffic from a range of IP addresses to be forwarded. Initially, this IP address range was set to be 192.168.1.101 – 192.168.1.102, which does not include any devices in the system. Figure 4 shows a screenshot of this security policy from the SmartDashboard GUI. Check Point R75 also creates implied rules, which are included in the security policy. Implied rules

[6] See pp. 10–11, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

[7] See, generally, pp. 28–29, "Check Point R75 Security Management Server Administration Guide" (dated Dec 15, 2010); see also p. 9 "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010): "Granular security policy control is possible by applying specific rules to specific gateways."

enable certain connections to occur to and from the security gateways using a variety of different services. One such rule that is always included is the Last Implied Rule, or "the default rule, which typically rejects all packets without logging."[8] The Last Implied Rule thus will cause packets from IP addresses outside the explicit range of allowed IP addresses to be dropped. A Cleanup Rule can also be included, which, like the Last Implied Rule, drops all traffic that is not permitted by the previous rules and allows logging.[9] A Cleanup Rule was not included in the tested configuration's security policy.

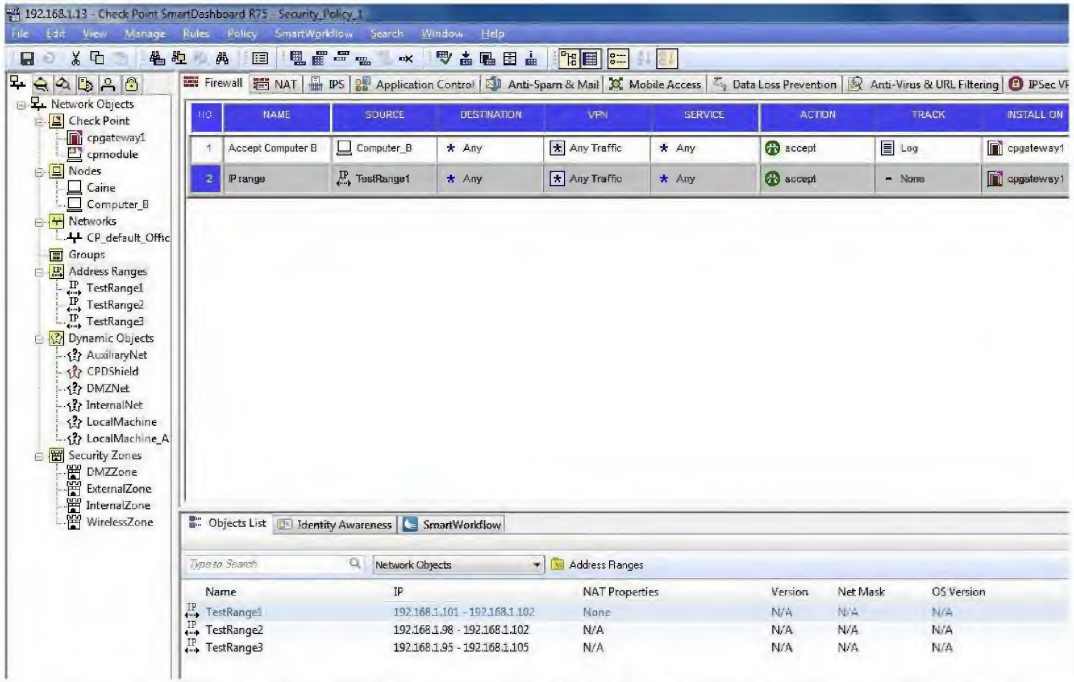


Figure 4: Screenshot of SmartDashboard GUI showing security policy with two explicit rules. The range of IP addresses

[8] See p. 11, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).
[9] See pp. 11–12, "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010).

CENTRIPETAL-CSCO 087914

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 414

allowed by the second rule is 192.168.1.101 – 192.168.1.102.

As shown in the screenshot in Figure 5, this policy was installed on Security Gateway 1. (The hostname of Security Gateway 1 is "cpgateway1," as seen on the right side of Figure 4.)

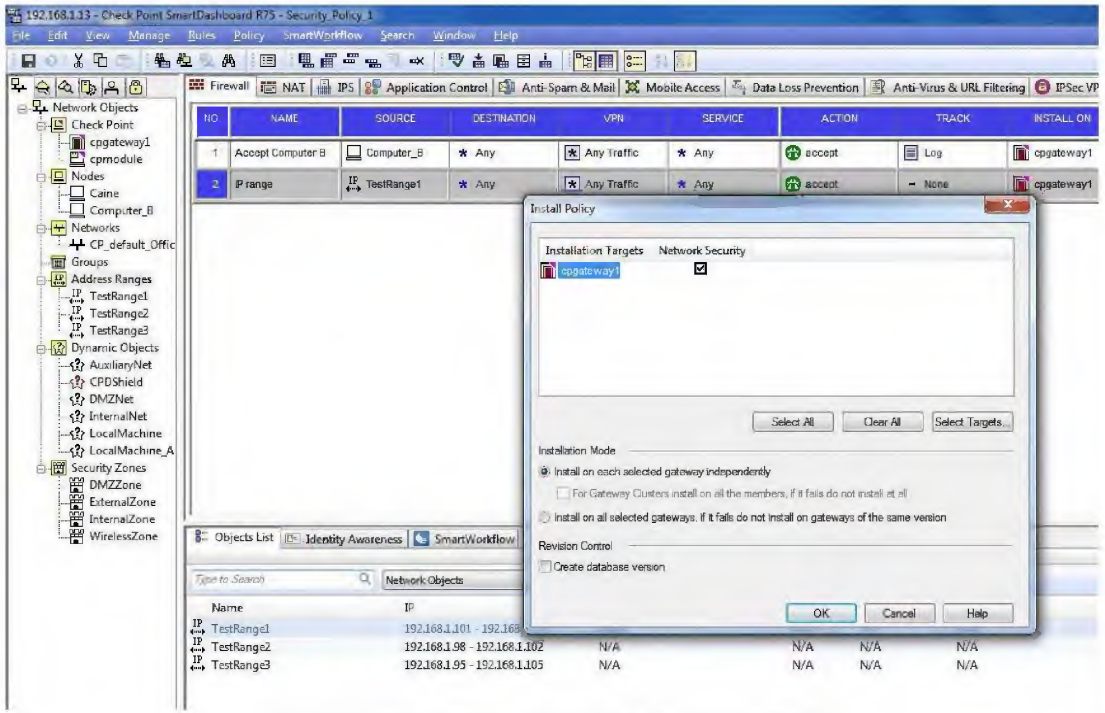


Figure 5: Installation of security policy on Security Gateway 1.

The security policy installation proceeded to completion with no errors (see Figure 6).[10]

[10] The installation completed with no errors and one warning that "anti-spoofing" was not configured. Anti-spoofing, which is not configured for our test setup, is described, for example, on page 14 of the "Check Point R75 Firewall Administration Guide" document.

CENTRIPETAL-CSCO 087915

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 415

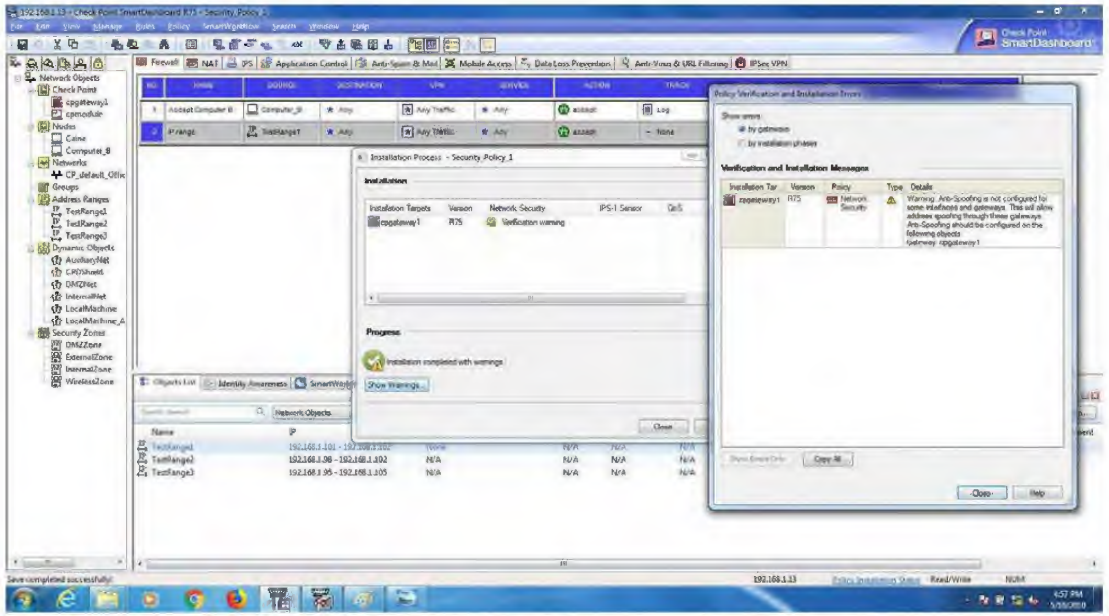


Figure 6: Dialog boxes indicating that the installation of the security policy completed. The clock in the lower right corner of the figure shows that this policy was installed around 4:57 pm, according to the internal clock on the SMS computer.

To demonstrate the operation of the security policy, Exponent attempted to send traffic from Computer A, whose IP address is outside the allowed range of Rule 2, to Computer B through Security Gateway 1.

First, Exponent attempted to ping Computer B from Computer A (see Figure 7). Using tcpdump to monitor traffic on interface eth0 of SG 1, incoming packets from Computer A (192.168.1.100) were observed:

Table 1: Incoming traffic from Computer A observed via the "tcpdump" utility on SG 1. No ICMP echo reply was observed.

`16:58:24.005864 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)`
`16:58:25.014620 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)`

CENTRIPETAL-CSCO 087916

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 416

These packets were dropped by SG 1 before they reached Computer B (172.16.1.99).



Figure 7: Screenshot of ping from Computer A ("exponent-laptop") to Computer B (172.16.1.99) indicating 100% packet loss, demonstrating that the security gateway dropped the packets.

As a second demonstration of the security policy functionality, Exponent also used the computer program "netcat" to attempt to establish a connection between Computer A and Computer B. While listening with "netcat" on Computer B, a test packet of text ("test_packet") was sent from Computer A to Computer B (see Figure 8 and Figure 9). The packet was not received by Computer B.

CENTRIPETAL-CSCO 087917

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 417

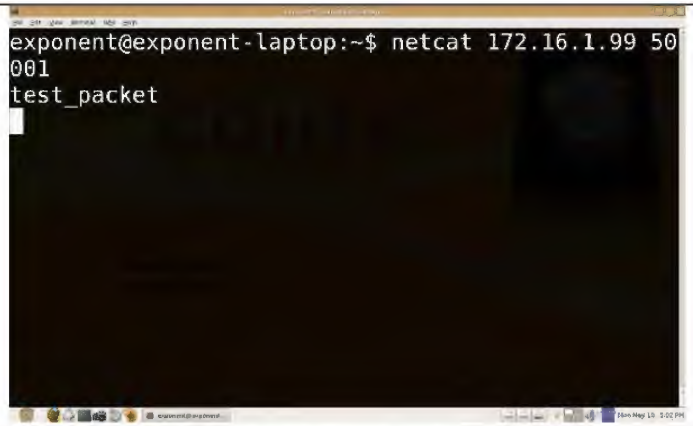


Figure 8: Sending packet of text ("test_packet") from Computer A ("exponent-laptop") to Computer B (172.16.1.99) on port 50001.

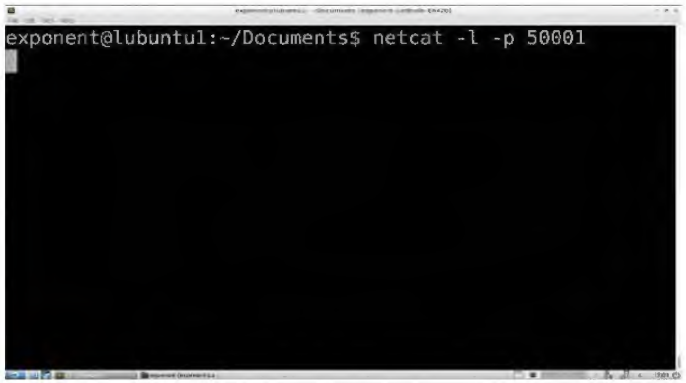


Figure 9: Listening for a packet of text ("test_packet") from Computer A on port 50001 on Computer B. No packet was received.

Thus, it has been demonstrated that this security policy includes at least one rule specifying a set of network addresses for which associated packets should be forwarded (explicit Rule 1 and Rule 2) and

	at least one rule specifying that all packets associated with network addresses outside that set of network addresses should be dropped (the Last Implied Rule). Based on Exponent's analysis of network traffic and the Check Point documentation, the Last Implied Rule drops all packets associated with network addresses outside the set of network addresses for which packets should be forwarded.
17d. receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	As configured Figure 3, the security gateway SG 1 receives, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded. At 4:57 pm, as recorded by the clock on the SmartDashboard GUI, [11] Security Gateway 1 received the dynamic security policy outlined in section 17c. This policy specified a set of network addresses for which packets should be forwarded: 192.168.1.101 – 192.168.1.102. Thus, it has been demonstrated that a dynamic security policy specifying a set of network addresses for which packets should be forwarded was received at a first time.
17e. receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	As configured in Figure 3, the security gateway SG 1 recieves, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded. As shown in Figure 10, at 5:04 pm (as recorded by the clock on the computer running the SmartDashboard GUI), Security Gateway 1 received a security policy with a second set of network addresses for which packets should be forwarded, contained in Rule 2: 192.168.1.98 – 192.168.1.102. This range includes more network addresses than the range in the security policy in claim element 17d. The time at which this second security policy was installed was later than the time at which the first security policy was installed.

[11] See Figure 6.

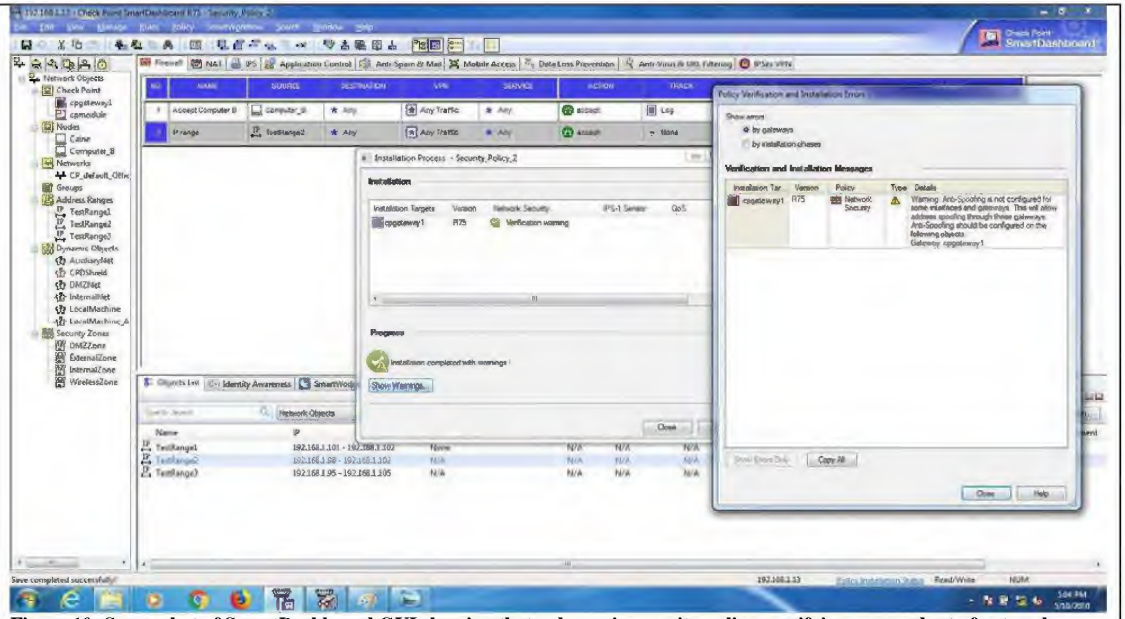


Figure 10: Screenshot of SmartDashboard GUI showing that a dynamic security policy specifying a second set of network addresses for which packets should be forwarded was received by Security Gateway 1 at 5:04 pm.

The range of network addresses that should be forwarded according to Rule 2 in this second security policy now includes the address of Computer A (192.168.1.100).

To demonstrate the operation of Rule 2, Exponent attempted to send packets from Computer A to Computer B. Rule 2 should allow forwarding of this traffic.

First, Exponent attempted to ping Computer B from Computer A (see Figure 11). Using tcpdump to monitor traffic on interface eth0 of SG 1, we observed request packets from Computer A (192.168.1.100) and response packets from Computer B (172.16.1.99), indicating that SG 1 was forwarding packets from Computer A to Computer B, as required by Rule 2:

CENTRIPETAL-CSCO 087920

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 420

Table 2: Traffic between Computer A and Computer B as observed via the "tcpdump" utility on SG1.

17:04:37.877141 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)
17:04:37.878478 172.16.1.99 > 192.168.1.100: icmp: echo reply
17:04:38.876155 192.168.1.100 > 172.16.1.99: icmp: echo request (DF)
17:04:38.876775 172.16.1.99 > 192.168.1.100: icmp: echo reply



Figure 11: Screenshot of ping from Computer A ("exponent-laptop") to Computer B (172.16.1.99) indicating 0% packet loss, demonstrating that the security gateway forwarded the packets.

Next, "netcat" was used to establish a connection between Computer A and Computer B. While listening with "netcat" on Computer B, a test packet of text ("test_packet") was sent from Computer A to Computer B (see Figure 12 and Figure 13). This time, the packet was received by Computer B.

CENTRIPETAL-CSCO 087921

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 421

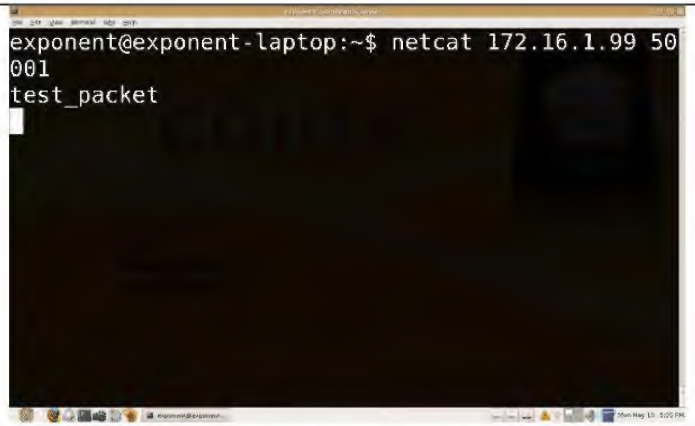


Figure 12: Sending packet of text ("test_packet") from Computer A ("exponent-laptop") to Computer B (172.16.1.99) on port 50001.

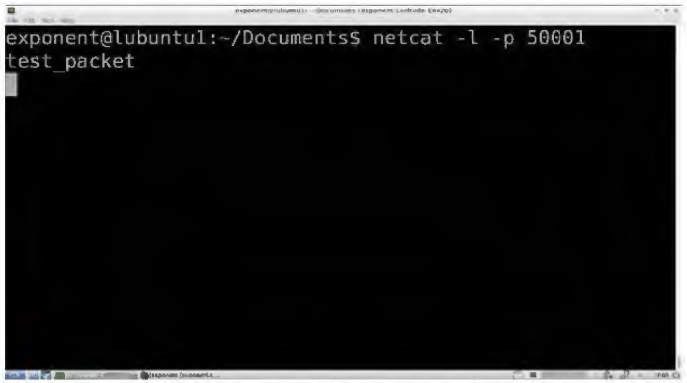


Figure 13: Listening on port 50001 on Computer B. One packet ("test_packet") was received from Computer A.

In addition, using tcpdump to monitor traffic on interface eth0 of SG 1, traffic was observed from Computer A (192.168.1.100) to Computer B (172.16.1.99). The observed data from the tpcdump utility also indicates that SG 1 was forwarding packets from Computer A to Computer B, as required

	by Rule 2: **Table 3: Traffic between Computer A and Computer B as observed via the "tcpdump" utility on SG1.** `17:05:29.842216 192.168.1.100.35948 > 172.16.1.99.50001: P 1:13(12) ack 1 win 46 <nop,nop,timestamp 64608257 2561232124> (DF)` `17:05:29.842726 172.16.1.99.50001 > 192.168.1.100.35948: . ack 13 win 227 <nop,nop,timestamp 2561236191 64608257> (DF)` Thus, it has been demonstrated that a dynamic security policy specifying a set of network addresses for which packets should be forwarded was received. Based on this analysis of network traffic and the Check Point documentation, Rule 2 of this security policy allows packets to be forwarded through the security gateway.
17f. receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;	As configured in Figure 3, the security gateway SG 1 receives, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses. As shown in Figure 14, at 5:08 pm (as recorded by the clock on the computer running the SmartDashboard GUI), Security Gateway 1 received a security policy with a third set of network addresses for which packets should be forwarded: 192.168.1.95 – 192.168.1.105. This range includes more network addresses than the range in the security policy in 17e.

CENTRIPETAL-CSCO 087923

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 423

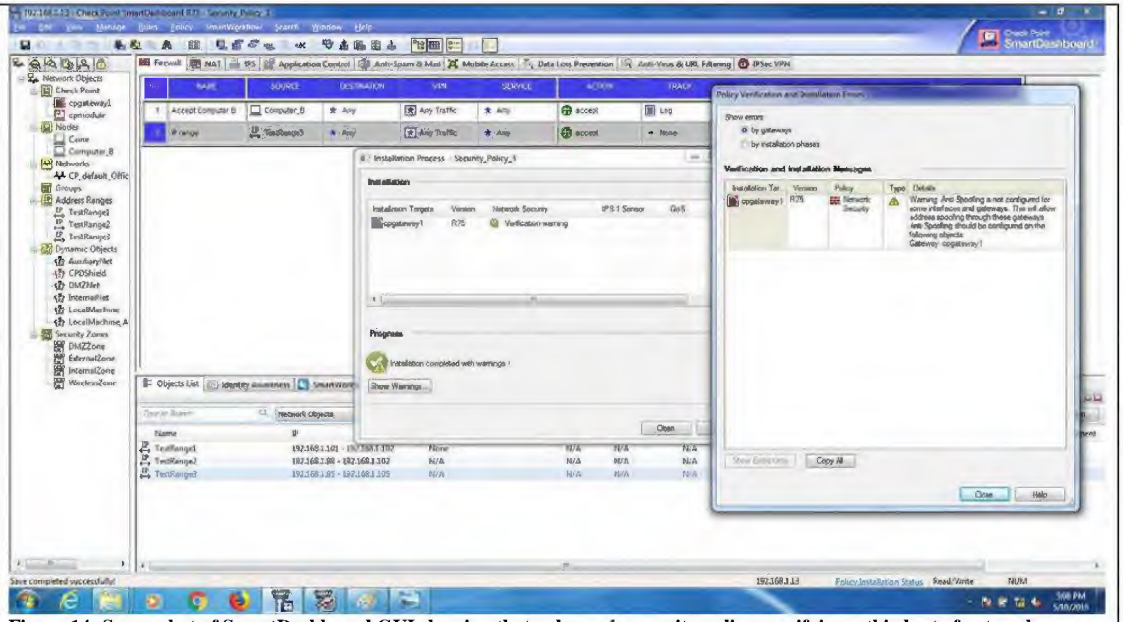


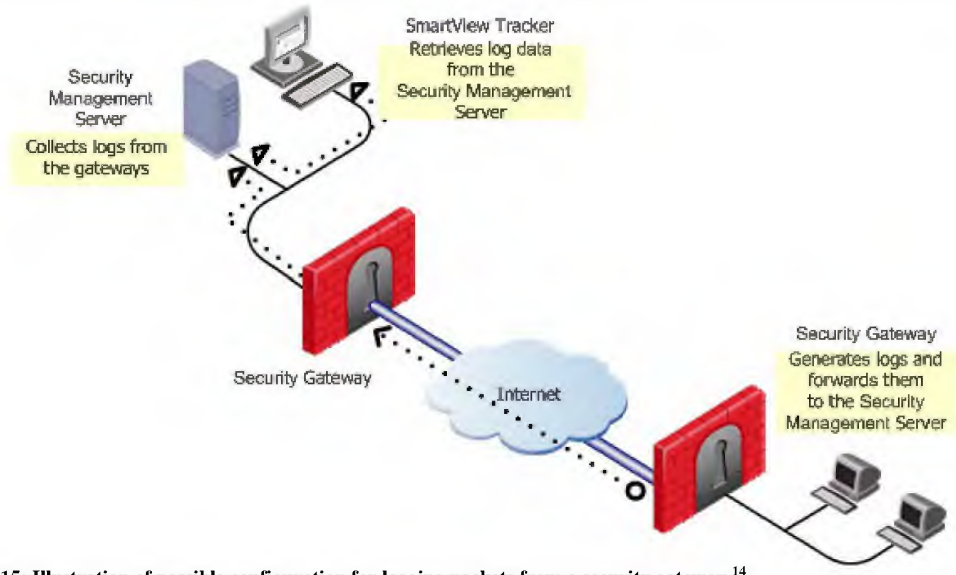
Figure 14: Screenshot of SmartDashboard GUI showing that a dynamic security policy specifying a third set of network addresses for which packets should be forwarded was received by Security Gateway 1 at 5:08 pm.

The screen captures of the SmartDashboard GUI shown in Figure 6, Figure 10, and Figure 14 have demonstrated that the security gateway SG 1 received three dynamic security policies. The first policy forwarded packets in the range 192.168.1.101 –192.168.1.102, the second policy forwarded packets in the range 192.168.1.98 – 192.168.1.102, and the third policy forwarded packets in the range 192.168.1.95 – 192.168.1.105. The first policy was received at 4:57 pm, the second policy was received at 5:04 pm, and the third policy was received at 5:08 pm.

Thus, it has been demonstrated that the second policy was received after the first policy, and the third policy was received after the second policy. Further, it has been demonstrated that the second set of network addresses included more network addresses than the first set, and the third set of network addresses included more network addresses than the second set.

17g. receive packets associated with a network protected by the packet security gateway;	As configured in Figure 2 and Figure 3, the security gateway SG 1 receives packets associated with a network protected by the packet security gateway. As was shown in claim element 17e using tcpdump, SG 1 received packets associated with Network B, which is the network protected by SG 1. Specifically, these packets were associated with Network B because their destination, Computer B, was within Network B. Thus, it has been demonstrated that in the Check Point R75 system, the security gateway receives packets associated with a network protected by the packet security gateway.
17h. and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other	As configured in Figure 3, the security gateway SG 1 performs, on a packet-by-packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein performing at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets. As stated in the patent, routing a packet to a monitoring device is an example of a packet transformation function other than forwarding or dropping.[12] As shown in Figure 15, the Check Point R75 system has the ability to log information about network traffic.[13] For each rule in the rule base, matching events can be tracked. The gateways collect and send data to the security management server, which makes logs available for inspection via SmartView Tracker. This logging process is a packet transformation function other than forwarding or dropping packets because it is a function applied to all packets that does not forward or drop packets. If a packet matches a rule from the rule base for which logging is activated, and the log does not already contain an event corresponding to that rule, and any other logging criteria are met, then some information from that packet will be logged.

[12] '205 Patent, Column 7, Lines 27–36.
[13] See p. 65, "Check Point R75 Security Management Administration Guide" (dated Dec 15, 2010).

than forwarding or dropping the packets.	 **Figure 15: Illustration of possible configuration for logging packets from a security gateway.**[14] All three security policies that were installed on SG 1 tracked events corresponding to Rule 1 by logging (See red box in Figure 16 showing logging in the third security policy, which was referenced in claim element 17f). Rule 1 allows traffic whose source is Computer B.

[14] See p. 65, "Check Point R75 Security Management Administration Guide" (dated Dec 15, 2010).

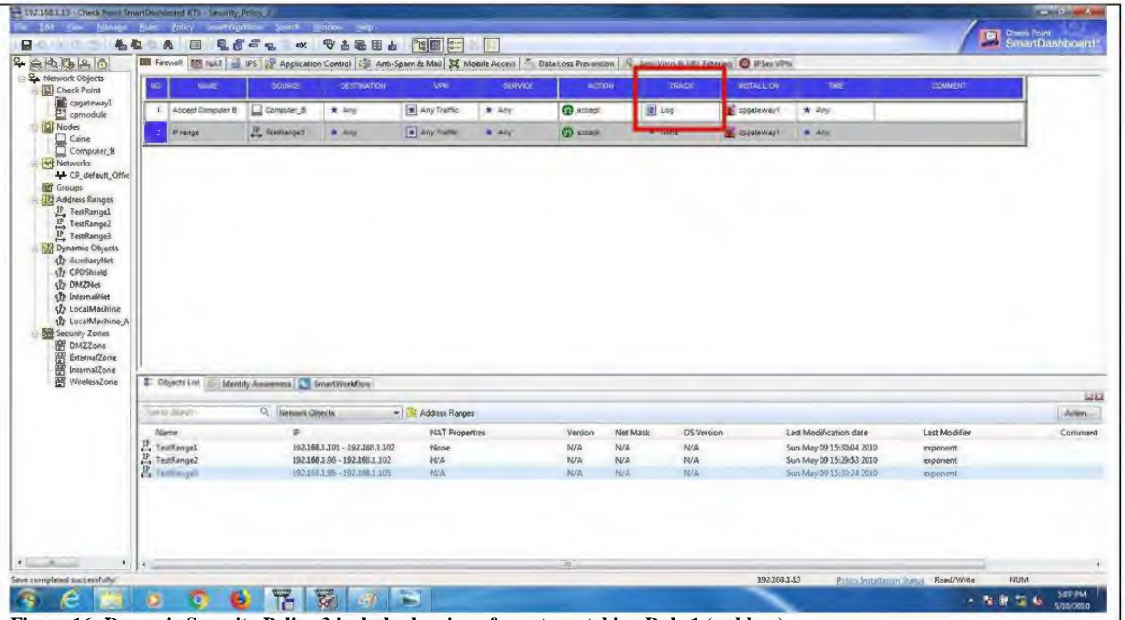


Figure 16: Dynamic Security Policy 3 includes logging of events matching Rule 1 (red box).

While the third security policy was installed on SG 1, logs were saved on the security management server and accessed using the SmartView Tracker on the GUI computer (see Figure 17).

CENTRIPETAL-CSCO 087927

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 427

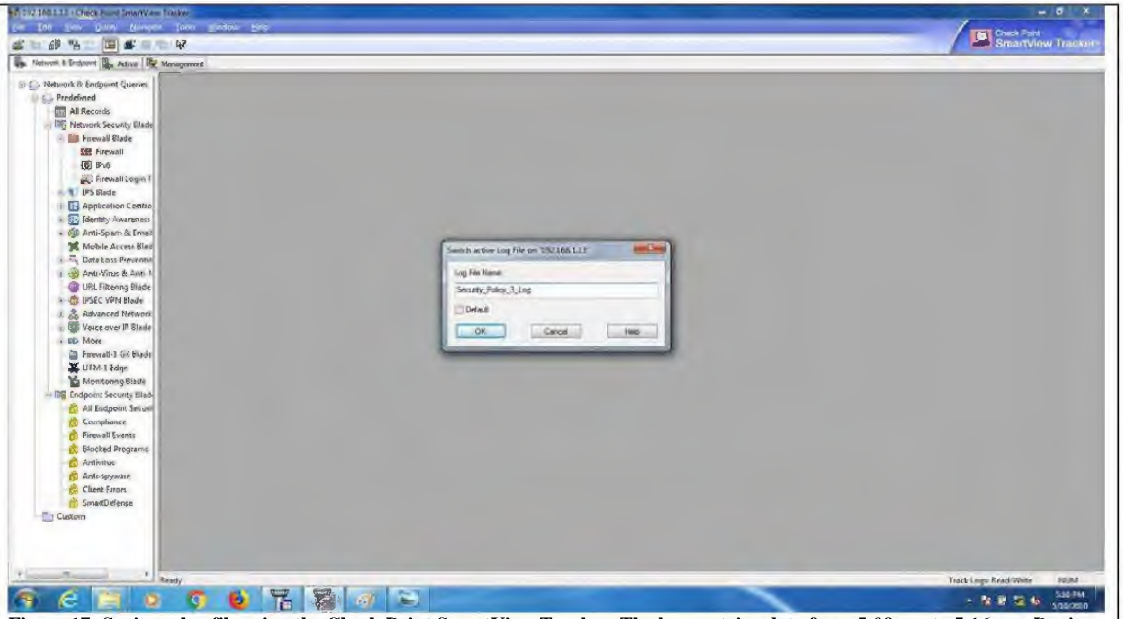


Figure 17: Saving a log file using the Check Point SmartView Tracker. The log contains data from 5:09 pm to 5:16 pm. During this time, the third dynamic security policy was installed on SG 1.

While logging was occurring, "netcat" was used to open a connection between Computer A and Computer B. Listening on Computer A, a test packet of text ("test_packet") was sent from Computer B on port 50001 (see Figure 18 and Figure 19). Another connection was then opened on port 50002 and used to send another test packet ("test_packet_2"). Both packets were received by Computer A.

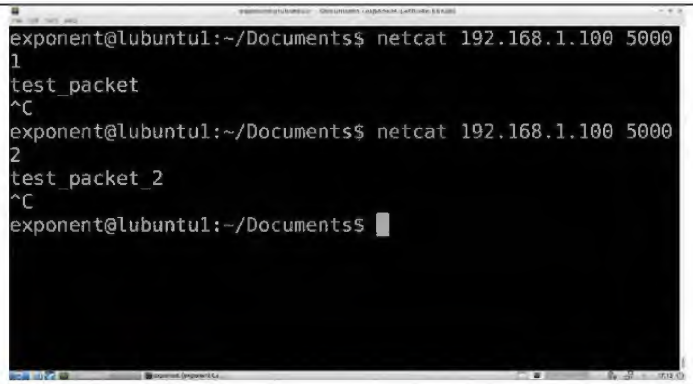


Figure 18: Sending packet of text ("test_packet") from Computer B ("lubuntu1") to Computer A (192.168.1.100) on port 50001 and then another packet ("test_packet_2") on port 50002.

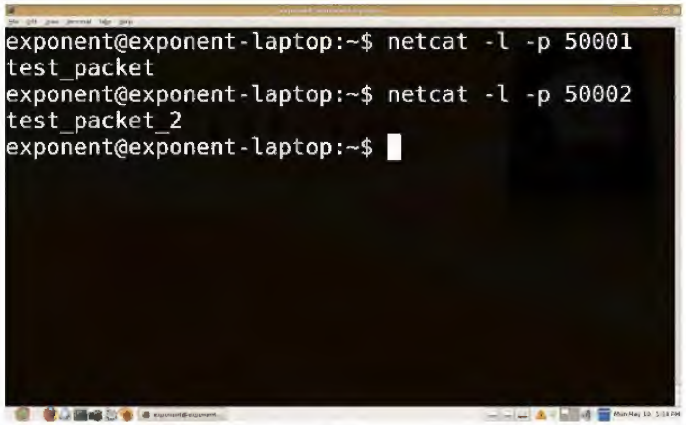


Figure 19: Listening for packets on port 50001 on Computer A ("exponent-laptop") and then on port 50002. One test packet was received on each port.

Using tcpdump to monitor traffic on interface eth0 of SG 1, SYN packets (highlighted in cyan in Table 4) from Computer B were observed each time a connection was opened (at 17:13:04.4239 and

at 17:13:33.3329). Data packets (highlighted in yellow in Table 4) from Computer B were also observed each time a packet of text was sent from Computer B to Computer A (at 17:13:11.4746 and 17:13:43.1192).

Table 4: Traffic between Computer A and Computer B as observed via the "tcpdump" utility on SG1.

17:13:04.423911 172.16.1.99.45672 > 192.168.1.100.50001: S 3985798800:3985798800(0) win 29200 <mss 1460,sackOK,timestamp 2561690808 0,nop,wscale 7> (DF)
17:13:04.424489 192.168.1.100.50001 > 172.16.1.99.45672: S 1009837749:1009837749(0) ack 3985798801 win 5792 <mss 1460,sackOK,timestamp 64721913 2561690808,nop,wscale 7> (DF)
17:13:04.425094 172.16.1.99.45672 > 192.168.1.100.50001: . ack 1 win 229 <nop,nop,timestamp 2561690810 64721913> (DF)
17:13:11.474583 172.16.1.99.45672 > 192.168.1.100.50001: P 1:13(12) ack 1 win 229 <nop,nop,timestamp 2561697860 64721913> (DF)
17:13:11.474972 192.168.1.100.50001 > 172.16.1.99.45672: . ack 13 win 46 <nop,nop,timestamp 64723676 2561697860> (DF)
17:13:18.580028 172.16.1.99.45672 > 192.168.1.100.50001: F 13:13(0) ack 1 win 229 <nop,nop,timestamp 2561704966 64723676> (DF)
17:13:18.580638 192.168.1.100.50001 > 172.16.1.99.45672: F 1:1(0) ack 14 win 46 <nop,nop,timestamp 64725453 2561704966> (DF)
17:13:18.581088 172.16.1.99.45672 > 192.168.1.100.50001: . ack 2 win 229 <nop,nop,timestamp 2561704967 64725453> (DF)
17:13:33.332870 172.16.1.99.44628 > 192.168.1.100.50002: S 2710554287:2710554287(0) win 29200 <mss 1460,sackOK,timestamp 2561719719 0,nop,wscale 7> (DF)
17:13:33.333346 192.168.1.100.50002 > 172.16.1.99.44628: S 1478261631:1478261631(0) ack 2710554288 win 5792 <mss 1460,sackOK,timestamp 64729141 2561719719,nop,wscale 7> (DF)
17:13:33.333920 172.16.1.99.44628 > 192.168.1.100.50002: . ack 1 win 229 <nop,nop,timestamp 2561719721 64729141> (DF)
17:13:43.119155 172.16.1.99.44628 > 192.168.1.100.50002: P 1:15(14) ack 1 win 229 <nop,nop,timestamp 2561729506 64729141> (DF)
17:13:43.119668 192.168.1.100.50002 > 172.16.1.99.44628: . ack 15 win 46 <nop,nop,timestamp 64731588 2561729506> (DF)
17:14:10.850280 172.16.1.99.44628 > 192.168.1.100.50002: F 15:15(0) ack 1 win 229 <nop,nop,timestamp 2561757240 64731588> (DF)
17:14:10.850728 192.168.1.100.50002 > 172.16.1.99.44628: F 1:1(0) ack 16 win 46 <nop,nop,timestamp 64738521 2561757240> (DF)

CENTRIPETAL-CSCO 087930

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 430

```
17:14:10.851156 172.16.1.99.44628 > 192.168.1.100.50002: . ack 2 win 229
<nop,nop,timestamp 2561757241 64738521> (DF)
```

The opening of these two connections was logged (see log file in Figure 20).

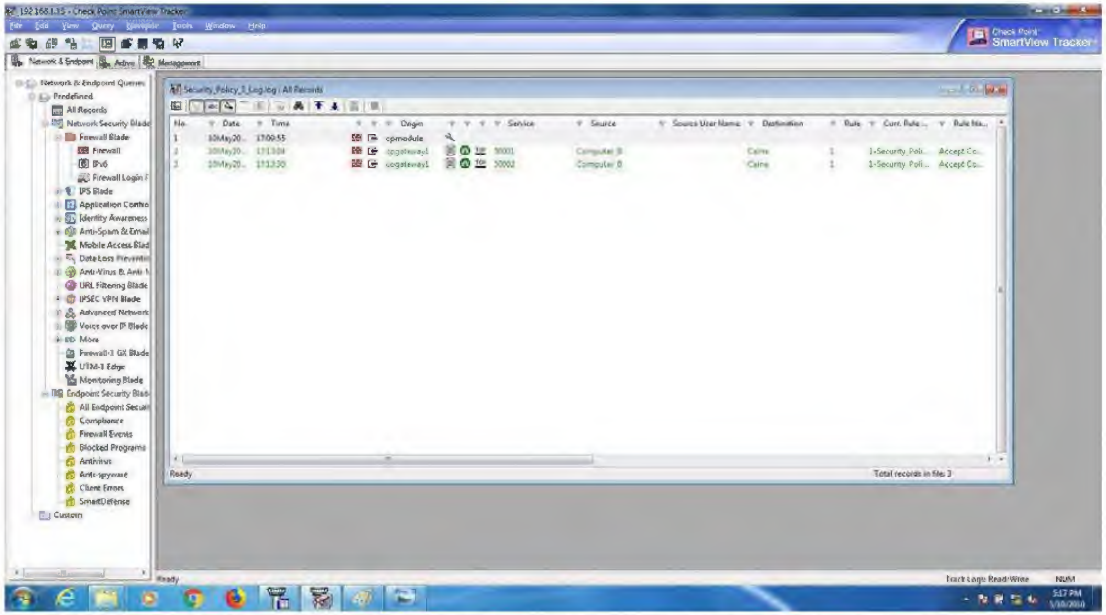


Figure 20: Log file containing data from 5:09 pm to 5:16 pm. During this time, the third dynamic security policy was installed on SG 1. Three events are recorded in the log. Event 1 records changing the name of the log file. Event 2 records opening the connection from Computer B on port 50001. Event 3 records opening the connection from Computer B on port 50002.

As shown in Figure 21, information from the SYN packets was recorded in the log.

CENTRIPETAL-CSCO 087931

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 431

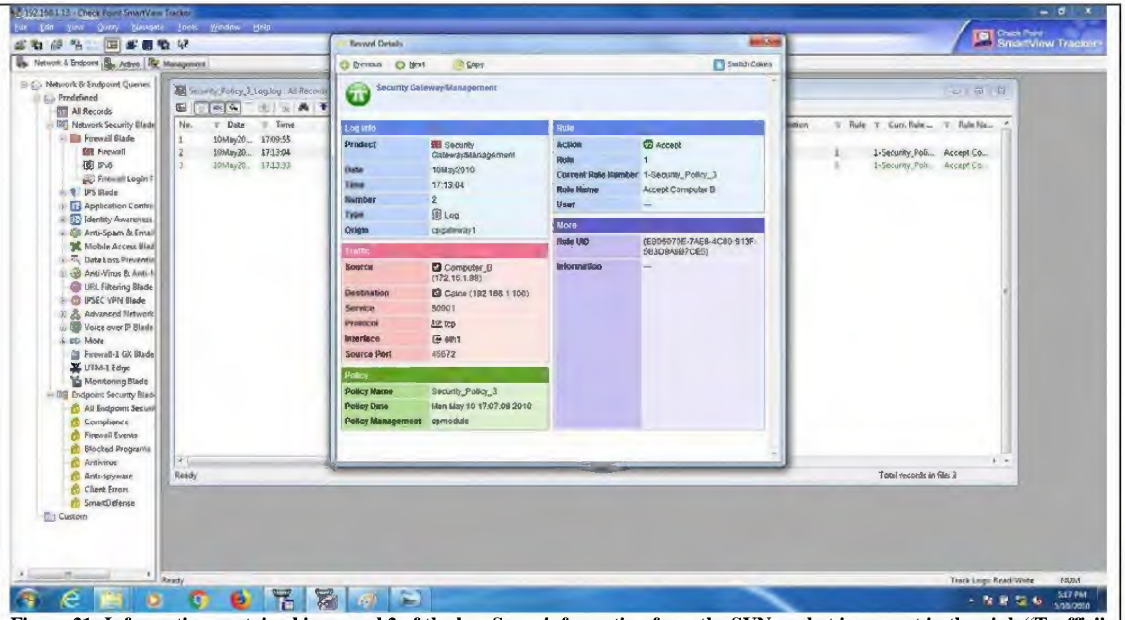


Figure 21: Information contained in record 2 of the log. Some information from the SYN packet is present in the pink "Traffic" table, indicating that a packet transformation function other than forwarding or dropping was performed.

The Check Point R75 system also includes monitoring, which, similar to logging, applies packet transformation functions other than forwarding or dropping.[15]

Thus, it has been demonstrated that the Check Point R75 system includes logging, and that logging is a packet transformation function other than forwarding or dropping that occurred in all three dynamic security policies installed on SG 1 on packets associated with Network B.

[15] See pp. 99 and 110 "Check Point R75 Firewall Administration Guide" (dated Dec 15, 2010). See also "Check Point R75 SmartView Monitor Administration Guide" (dated 17 April 2013).

Claim 33 Analysis

Claim 33	Analysis of Check Point R75
33a. One or more non-transitory computer readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:	The tested Check Point R75 installation has one or more non-transitory computer readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to execute claim elements 33b, 33c, 33d, 33e, 33f, 33g, and 33h. As discussed in the analysis of Claim 17, the tested Check Point R75 installation comprises two Dell PowerEdge 1750 computers functioning as packet security gateways that are both associated with a security policy management server. The Dell PowerEdge 1750 computers contain hard drives, which are non-transitory computer readable media. These hard drives have instructions stored on them that, when executed, cause each packet security gateway to perform the functionality specified in claim elements 33b, 33c, 33d, 33e, 33f, 33g, and 33h.
33b. receive a plurality of dynamic security policies from the security policy management server;	The tested Check Point R75 installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive a plurality of dynamic security policies from the security policy management server. See claim element 17b.
33c. receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with	The tested Check Point R75 installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped. See claim element 17c.

network addresses outside the set of network addresses for which packets should be forwarded should be dropped;	
33d. receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	The tested Check Point R75 installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded. See claim element 17d.
33e. receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	The tested Check Point R75 installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded. See claim element 17e.
33f. receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses	The tested Check Point R75 installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses. See claim element 17f.

including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;	
33g. receive packets associated with a network protected by the packet security gateway;	The tested Check Point R75 installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to receive packets associated with a network protected by the packet security gateway. See claim element 17g.
33h. and perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the	The tested Check Point R75 installation has media of claim element 33a, having instructions stored thereon, that when executed, cause each packet security gateway to perform, on a packet-by-packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets. See claim element 17h.

plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.	

CENTRIPETAL-CSCO 087936

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 436

APPENDIX D

'722 Patent Analysis

TippingPoint

Contents

Claim 1 Analysis 1
Claim 25 Analysis 18

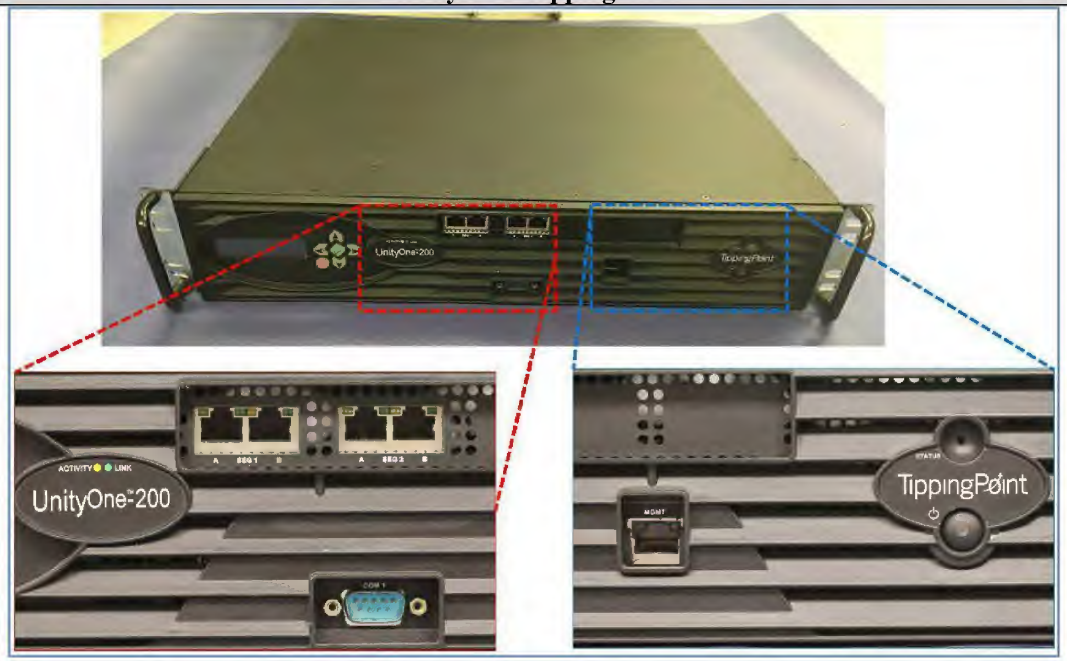
CENTRIPETAL-CSCO 087938

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 438

Claim 1 Analysis

Claim 1	Analysis of TippingPoint
1a. A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;	The TippingPoint UnityOne-200 Intrusion Prevention System (hereinafter, "TippingPoint IPS" or "TippingPoint system") performs a method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators. The TippingPoint IPS is "an Intrusion Prevention System that provides a unified approach to network security."[1] The physical TippingPoint IPS device that was used to perform testing as part of these claim analyses is shown in Figure 1. This device has part number "SBASY-199 Rev: C03" and serial number "ST05170004," as shown in Figure 2.

[1] "TippingPoint IPS Hardware Installation and Safety Guide v 2.5.4" (copyright 2008) at p. xi.

Claim 1	Analysis of TippingPoint
	 **Figure 1: Annotated photographs of the TippingPoint IPS used in the test network. The red and blue dashed boxes and lines are annotations. The red call-out box shows the SEG1-A, SEG1-B, SEG2-A, and SEG2-B Ethernet ports as well as the UnityOne-200 model name. The blue call-out box shows the MGMT Ethernet port as well as the TippingPoint manufacturer name.**

Claim 1	Analysis of TippingPoint
	 **Figure 2: TippingPoint IPS hardware showing the part number and serial number of the device.** The TippingPoint IPS comprises a packet-filtering device, which can detect and block packets based on a variety of packet-filtering rules provided by the local security manager (LSM). These rules can be set from a graphical user interface (web client) on a computer connected to the MGMT interface of the TippingPoint IPS. Specifically, the SEG1-A and SEG1-B Ethernet ports shown in Figure 1 are inputs/outputs to a packet-filtering device that was used to test and verify the functionality described in Claim 1. The SEG2-A and SEG2-B Ethernet ports are inputs/outputs for a second packet-filtering device that was used to test and verify the functionality described in Claim 25.

Claim 1	Analysis of TippingPoint
	Additionally, the packet-filtering device can detect and block packets based on packet-filtering rules that correspond to specific network threat indicators. For example, the specific "filter" corresponding to the "HTTP: Protected File Access" network threat is shown in Figure 3. Based on the description of the threat given in Figure 3 and based on Exponent's testing, we determined that this specific "filter" will block packets containing HTTP requests for the file "/etc/passwd."

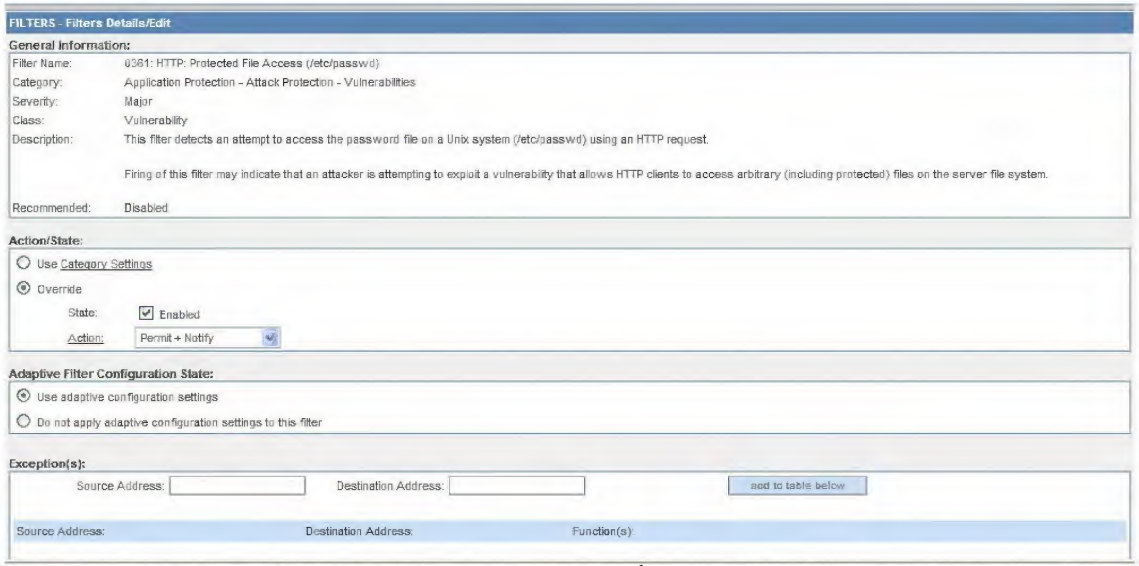


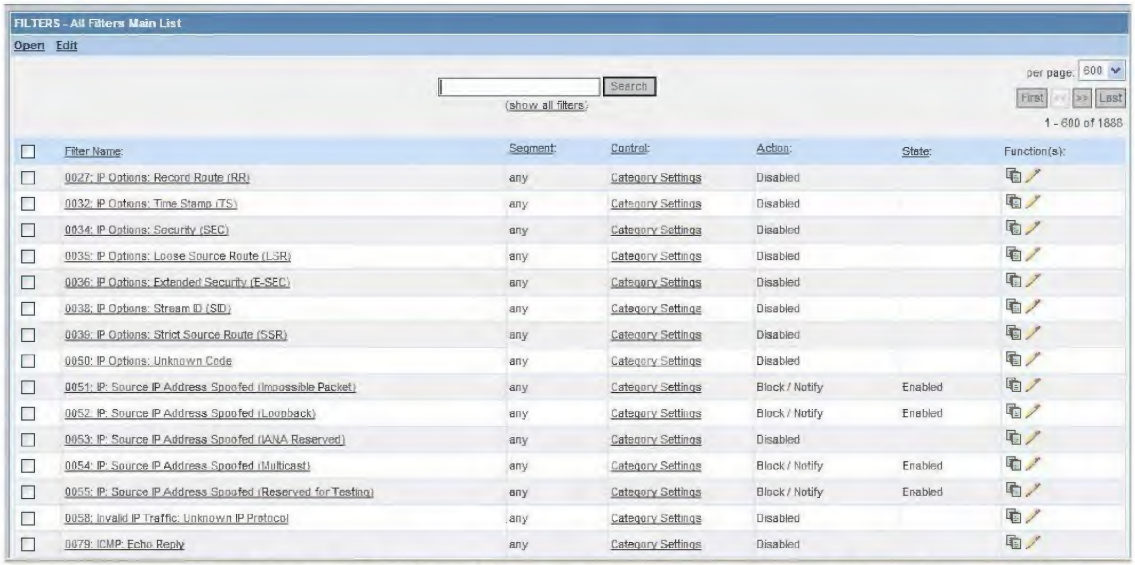
Figure 3: Screenshot from the TippingPoint LSM graphical user interface[2] display of the description of filter "0361," which "detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request."

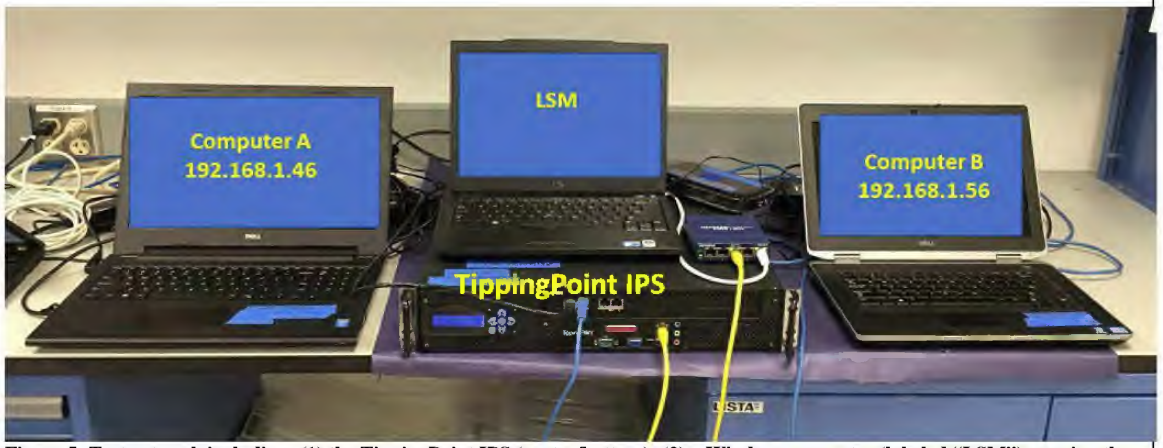
Figure 3 shows the following description for filter 0361: "This filter detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request. Firing of this filter may indicate that an attacker is attempting to exploit a vulnerability that allows HTTP clients to access arbitrary

[2] See, generally, "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005).

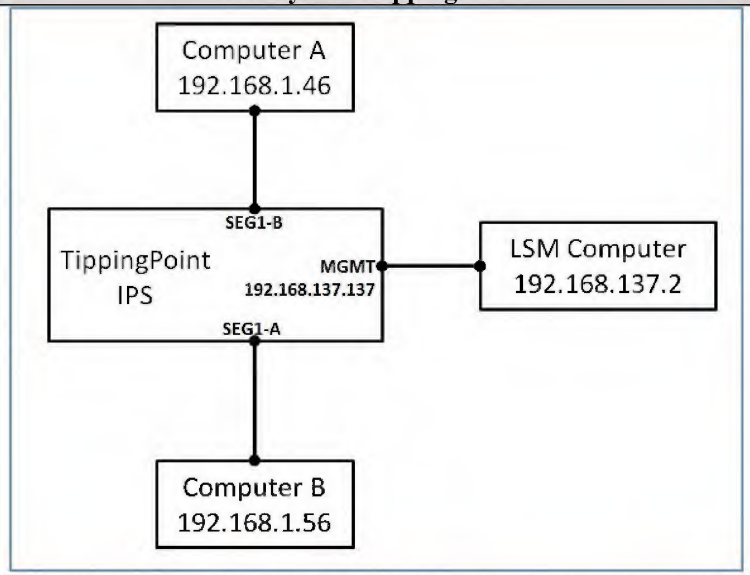
CENTRIPETAL-CSCO 087942

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 442

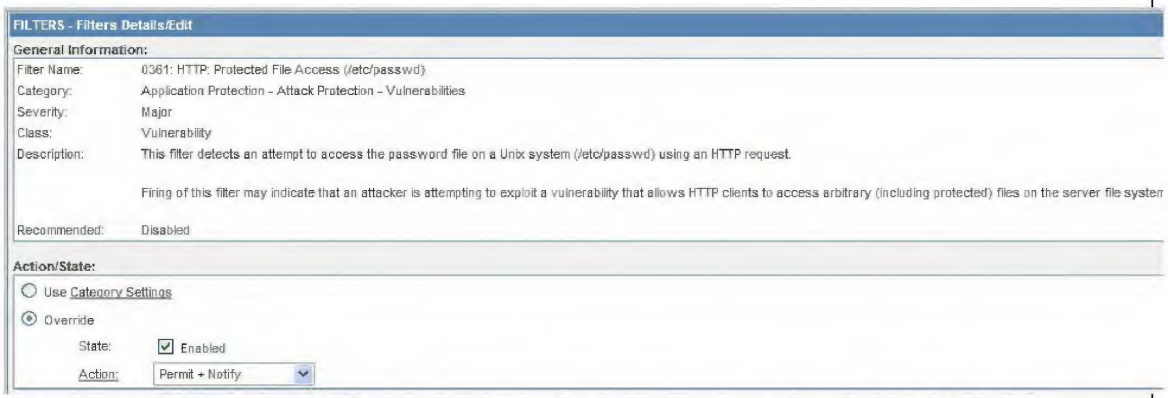
Claim 1	Analysis of TippingPoint
	(including protected) files on the server file system." Certain operating systems store sensitive information such as user passwords in the file "passwd" in the "/etc" directory, for which the full path is "/etc/passwd." Certain vulnerable web servers may allow data exfiltration attacks such as directory traversal attacks on the sensitive data in this file from remote (networked) locations. These attacks are initiated via a request packet that contains the string "/etc/passwd." Therefore, the rule to block HTTP requests containing the string "/etc/passwd" is a packet-filtering rule that corresponds to this network threat of protected file access via the web. The TippingPoint IPS can filter packets based on many different packet-filtering rules in addition to the rule shown in Figure 3. These rules are used to identify numerous different network threats, some of which are shown in Figure 4.  FILTERS - All Filters Main List Open Edit Search (show all filters) per page: 600 First << >> Last 1 - 600 of 1888 Filter Name: Segment: Control: Action: State: Function(s): 0027: IP Options: Record Route (RR) any Category Settings Disabled 0032: IP Options: Time Stamp (TS) any Category Settings Disabled 0034: IP Options: Security (SEC) any Category Settings Disabled 0035: IP Options: Loose Source Route (LSR) any Category Settings Disabled 0036: IP Options: Extended Security (E-SEC) any Category Settings Disabled 0038: IP Options: Stream ID (SID) any Category Settings Disabled 0039: IP Options: Strict Source Route (SSR) any Category Settings Disabled 0050: IP Options: Unknown Code any Category Settings Disabled 0051: IP: Source IP Address Spoofed (Impossible Packet) any Category Settings Block / Notify Enabled 0052: IP: Source IP Address Spoofed (Loopback) any Category Settings Block / Notify Enabled 0053: IP: Source IP Address Spoofed (IANA Reserved) any Category Settings Disabled 0054: IP: Source IP Address Spoofed (Multicast) any Category Settings Block / Notify Enabled 0055: IP: Source IP Address Spoofed (Reserved for Testing) any Category Settings Block / Notify Enabled 0058: Invalid IP Traffic: Unknown IP Protocol any Category Settings Disabled 0079: ICMP: Echo Reply any Category Settings Disabled **Figure 4: Screenshot from the TippingPoint LSM graphical user interface display of available filters and their current state of implementation.**

Claim 1	Analysis of TippingPoint
	The TippingPoint IPS "provides… monitoring and managing packets while blocking malicious attacks… provides total packet inspection… integrates Intrusion Prevention, Stateful IP Filtering (traffic management filters), and network discovery security applications into a device…"[3] The TippingPoint IPS "detects and blocks inappropriate, incorrect, or anomalous activity on the network by comparing network traffic with *filters*…"[4] (emphasis in original) The test network physical setup, including the TippingPoint IPS, is shown in Figure 5:  **Figure 5: Test network including: (1) the TippingPoint IPS (center/bottom); (2) a Windows computer (labeled "LSM") running the LSM graphical user interface (web client) that is connected to the management interface (center/top); (3) a Linux computer (labeled Computer A) connected to the SEG1-A packet filter input/output port; (4) a Windows computer (labeled Computer B) connected to the SEG1-B packet filter input/output port.** Figure 6 provides a schematic map of the test network.

[3] "TippingPoint IPS Hardware Installation and Safety Guide v 2.5.4" (copyright 2008) at p. 1.
[4] Ibid.

Claim 1	Analysis of TippingPoint
	 **Figure 6: Network map of test network illustrating connectivity of TippingPoint IPS, Computer A, Computer B, and LSM Computer.** As shown in Figure 5 and Figure 6, the test network includes a computer (Computer A) attached to Ethernet port SEG1-A and a computer (Computer B) attached to Ethernet port SEG1-B of the TippingPoint IPS. Traffic between Computer A and Computer B can be filtered by the TippingPoint IPS, as shown in more detail below. The test network also includes a computer (LSM Computer) that is used to connect to the TippingPoint IPS graphical user interface (GUI) called the Local Security Manager (LSM). The LSM "provides a graphical interface for on-the-box administration, configuration, and reporting."[5]

[5] "TippingPoint IPS Hardware Installation and Safety Guide v 2.5.4" (copyright 2008) at p. 2.

Claim 1	Analysis of TippingPoint
1b. receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	The TippingPoint system performs receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet. The TippingPoint IPS includes an "Alert Log," which shows suspicious packets that were allowed to be sent, and "Block Log," which shows packets that were blocked from transmission to the destination. The first packet tested included an HTTP GET request for the file "/etc/passwd." A packet containing this type of GET request will be filtered by the 0361 filter of the TippingPoint IPS introduced in Figure 3. At the beginning of testing, this filter was initially configured to "Permit + Notify" this type of network attack (see Figure 7). When the TippingPoint IPS filter is configured to "Permit + Notify" for a specific attack, the attack packet will be logged and allowed to pass.[6]  FILTERS - Filters Details/Edit General Information: Filter Name: 0361: HTTP: Protected File Access (/etc/passwd) Category: Application Protection - Attack Protection - Vulnerabilities Severity: Major Class: Vulnerability Description: This filter detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request. Firing of this filter may indicate that an attacker is attempting to exploit a vulnerability that allows HTTP clients to access arbitrary (including protected) files on the server file system Recommended: Disabled Action/State: Use Category Settings Override State: Enabled Action: Permit + Notify **Figure 7: Screenshot from the TippingPoint LSM GUI showing that the 0361 filter is set to the action "Permit + Notify."** To test this functionality of the TippingPoint IPS, we set up two computers, one to play the role of an

[6] "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005) at p. 72.

Claim 1	Analysis of TippingPoint
	HTTP client and one to play the role of an HTTP server. Computer B (see Figure 5 and Figure 6) at network IP address 192.168.1.56 was configured to host a HTTP server.[7] Computer A at network IP address 192.168.1.46 was used to make HTTP GET request to attempted to access the URL path "/etc/passwd" on the HTTP server. That is, Computer A played the role of a HTTP client. Initially, the TippingPoint IPS was configured to "Permit + Notify" for the 0361 filter, which corresponds to the "HTTP: Protected File Access" threat. While the TippingPoint IPS was configured to "Permit + Notify" this threat, a first packet, including an HTTP GET request for the URL path "/etc/passwd," was sent by Computer A to the IP address associated with Computer B. During this testing, the HTTP server on Computer B was configured to server web pages on port 8000 rather than port 80.[8] To send the HTTP GET request, we used the program "netcat." The netcat program is a well-known utility[9] for sending data using the TCP/IP protocol, which we used to send HTTP requests.[10] We used the netcat utility rather than a more complex web browser (e.g., Chrome or Internet Explorer) to have more fine-grained control over the test packets that were sent. A terminal window display from Computer A is shown in Figure 8. This figure shows (1) the use of netcat (the command line invocation of netcat is performed via the "nc" command) on Computer A to connect to port 8000 on Computer B (first line); (2) the HTTP GET request for the "etc/passwd" path (second line); (3) the HTTP response from the web server at Computer B indicating that the file was not found (remaining lines).

[7] Python programming language was used with a python language interpreter and standard python module called "http.server" to run an HTTP server on Computer B. For additional information, see https://docs.python/org (generally) as well as https://docs.python.org/2/library/simplehttpserver.html and https://docs.python.org/3/library/http.server.html.

[8] Port 8000 is the default port used by the python http server module.

[9] See, for example, http://netcat.sourceforge.net/ and https://nmap.org/ncat/.

[10] HTTP is an application layer protocol that typically runs on top of the lower-level TCP protocol.

Claim 1	Analysis of TippingPoint

```
exponent@adam-jumpkit:~$ nc 192.168.1.56 8000
GET /etc/passwd HTTP/1.1

HTTP/1.0 404 File not found
Server: SimpleHTTP/0.6 Python/3.4.2
Date: Wed, 30 May 2018 01:20:41 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Content-Length: 452

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 404</p>
        <p>Message: File not found.</p>
        <p>Error code explanation: 404 - Nothing matches the given URI.</p>
    </body>
</html>
```

Figure 8: Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, the HTTP GET request for the "/etc/passwd" path, and the response from Computer B indicating that the "etc/passwd" file was not found by the server (thus it responds with a 404 error).

Because the TippingPoint IPS was configured to "Permit + Notify" this threat, the HTTP GET request was allowed to pass from Computer A, through the TippingPoint IPS, and arrive at Computer B. The arrival of the HTTP GET request at Computer B is illustrated in Figure 9, which shows that the GET request for the path "/etc/passwd" invokes an HTTP code 404 response because the file "/etc/passwd" is not available on the HTTP server. The 404 response also appears back at the HTTP client on Computer A, as demonstrated in Figure 8.

```
C:\Users\Tester\Desktop\web>python -m http.server
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.46 - - [29/May/2018 18:20:41] code 404, message File not found
192.168.1.46 - - [29/May/2018 18:20:41] "GET /etc/passwd HTTP/1.1" 404 -
```

Figure 9: Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server has sent back an HTTP code 404 in response to the GET request for "/etc/passwd."

Claim 1	Analysis of TippingPoint
	As Figure 10 illustrates, the "Alert Log" on the LSM GUI records that the first packet was detected and allowed to continue to the destination.[11] Specifically, Figure 10 shows that the HTTP attack packet associated with the 0361 filter was received from the source 192.168.1.46 (Computer A) and allowed to continue to destination 192.168.1.56 (Computer B).



Figure 10: Screenshot from the TippingPoint LSM GUI showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was allowed.

Next, as Figure 11 shows, the TippingPoint IPS was configured to "Block + Notify" the same HTTP threat corresponding to the 0361 filter. Then a second packet, including an HTTP GET request for the URL path "/etc/passwd," was sent by Computer A to the IP address associated with Computer B.

[11] See "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005) section "Alert Log" starting on p. 115.

Claim 1	Analysis of TippingPoint

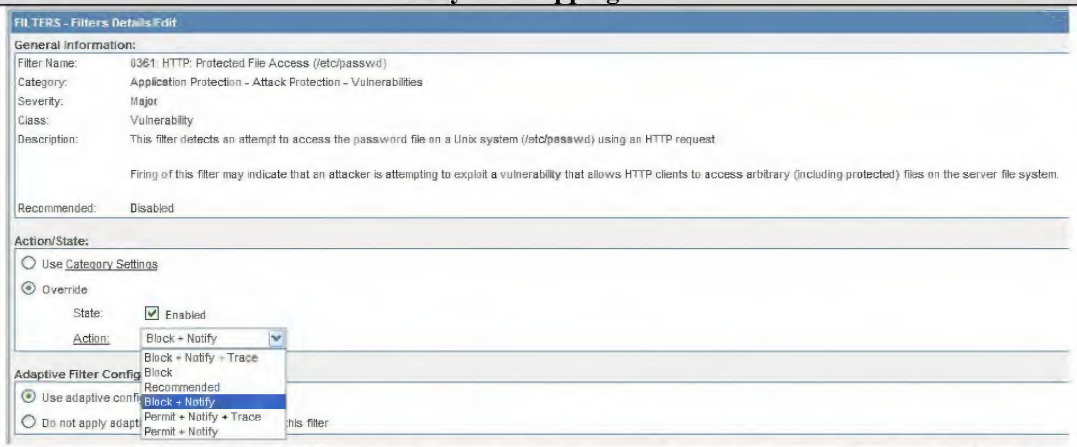


Figure 11: Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from "Permit + Notify" to "Block + Notify."

Figure 12 shows a terminal window display from Computer A. Specifically, it shows (1) the use of netcat (the command line invocation of netcat is performed via the "nc" command) on Computer A to connect to port 8000 on Computer B (first line); (2) the HTTP GET request for the "etc/passwd" path (second line); and (3) the absence of any HTTP response from the web server at Computer B and subsequent shutdown of the HTTP client using the "Ctrl-C" keyboard combination to send the client process a kill signal.

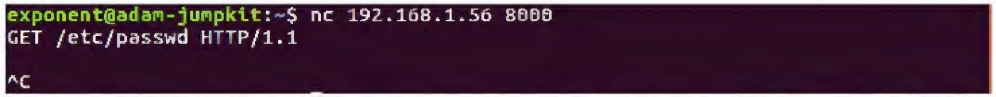
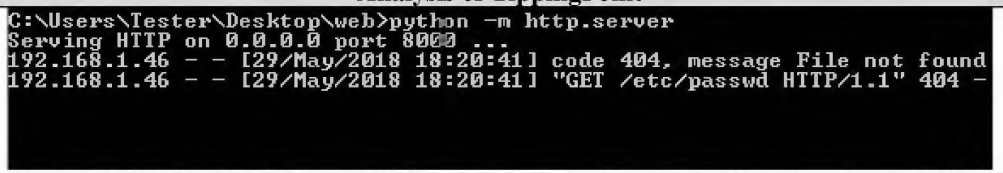


Figure 12: Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, and the HTTP GET request for the "/etc/passwd" path. It also illustrates that no response was received from Computer B (because Computer B never received the request).

Claim 1	Analysis of TippingPoint
	Figure 13 illustrates the "Block Log" on the LSM GUI, which shows that the second packet was detected and blocked by the TippingPoint IPS packet filter. [12] Specifically, Figure 13 shows that the HTTP attack packet associated with the 0361 filter was received from source 192.168.1.46 (Computer A) and blocked from continuing to destination 192.168.1.56 (Computer B).  LOGS - Block Log Open Edit per page: 50 First Freeze | Refresh in 16 1 - 1 of 1 Log ID: Date/Time: Severity: Filter Name: Protocol: Segment: Source Address: Dest Address: Packet Trace: Hit Count: 14 2010-05-29 18:22:35 Major 0361: HTTP: Protected File Access (/etc/passwd) http Segment 1 192.168.1.46:39004 192.168.1.56:8000 1 per page: 50 First 1 - 1 of 1 **Figure 13: Screenshot from the TippingPoint LSM GUI, showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was blocked. Note that the time recorded on the LSM GUI for this blocking action is 18:22:35, whereas the alert log shown in Figure 10 occurred roughly two minutes prior (at 18:20:39).** Because the TippingPoint IPS was configured to "Block + Notify" this HTTP file access threat prior to the arrival of the second packet, the HTTP GET request was *not* allowed to pass from Computer A through the TippingPoint IPS. Therefore, this packet never arrived at Computer B. The lack of arrival (i.e., being blocked) is illustrated in Figure 14, which shows the same text as Figure 9 in the Windows cmd terminal. The figure also shows additional whitespace, indicating that the request was not received; had the request been received, there would be a second code 404 response logged to the terminal windows as well as a second GET request logged to the terminal window; however, no such log lines were displayed.

[12] See "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005) section "Block Log" starting on p. 116.

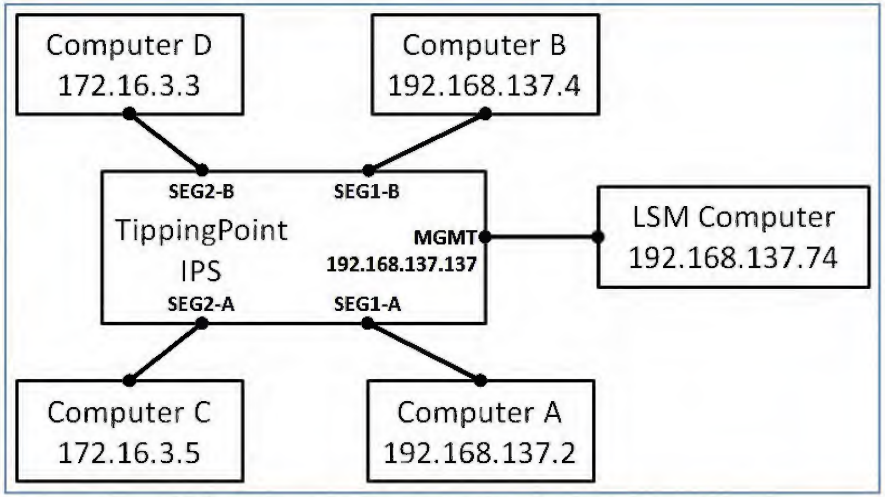
Claim 1	Analysis of TippingPoint
	 **Figure 14: Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server did not send back any additional response because it did not receive the second packet.(The response shown here is the response to the first packet that occurred at 18:20:41 on Computer B in Figure 9.)**
1c.responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators: applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet;	The TippingPoint system performs, responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators: applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet. As described above in the analysis of claim elements 1a and 1b, the first packet (from Computer A) was allowed to continue toward its destination (Computer B). See, for example, Figure 7 through Figure 10. Figure 7 shows that the TippingPoint IPS was configured to "Permit + Notify" regarding the HTTP protected file access attack corresponding to packet filter 0361. Figure 8 shows that the first packet was sent from Computer A toward the destination of Computer B. Figure 9 shows that the packet was received at the destination (Computer B); therefore, it was allowed to continue through the TippingPoint IPS. Figure 8 also confirms that the packet was allowed to continue, because Computer B received a response from the HTTP server. Figure 10 shows that the TippingPoint IPS logged the allowance of the packet corresponding to the HTTP protected file access network threat.

Claim 1	Analysis of TippingPoint
1d. communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;	The TippingPoint system performs communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet. As described above in the analysis of claim elements 1a, 1b, and 1c, the first packet (from Computer A) was allowed to continue toward its destination (Computer B). See, for example, Figure 7 through Figure 10. In particular, Figure 10 shows the Allow Log for the TippingPoint IPS, indicating that the packet was allowed. For the TippingPoint LSM GUI to display this log information to the user, the packet must have been allowed to continue and the packet-filtering device must have communicated this fact to a data store served by the web server running on the TippingPoint IPS management interface. It is this web server that provides the content that is viewable by a user running the LSM GUI (which includes a web client connected to the web server running on the management interface).
1e. causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;	The TippingPoint system performs causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators. As described above in the analysis of claim elements 1a, 1b, 1c, and 1d, the first packet (from Computer A) was allowed to continue toward its destination (Computer B). See, for example, Figure 7 through Figure 10. Furthermore, information regarding the packet was displayed in the LSM GUI, as shown in Figure 10, which displays information corresponding to the packet-filtering rule 0361 and the HTTP protected file access network threat, indicating that the packet associated with the threat was allowed to continue to its destination.
1f. receiving, by the packet-filtering device, an	The TippingPoint system performs receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the

Claim 1	Analysis of TippingPoint
instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and	packet-filtering rule and the one or more network-threat indicators. As described above in the analysis of claim element 1a and 1b, the first packet (from Computer A) was allowed to continue toward its destination (Computer B). See, for example, Figure 10, which shows that a packet associated with the HTTP protected file access threat was allowed. Furthermore, Figure 11 shows an element of a GUI (a drop-down menu) associated with this threat. This element is accessible to the user via the LSM and displays multiple options for how to handle packets corresponding to this rule and threat. When the handling option for this threat is changed from "Permit + Notify" to "Block + Notify" and the changes are saved, the packet-filtering device will receive an instruction to block the packet rather than to allow the packet. This is further illustrated in Figure 12, Figure 13, and Figure 14, which show that after this setting was changed in response to the user input the second packet was blocked.
1g. responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and	The TippingPoint system performs responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations. As described above in the analysis of claim element 1a and 1b, the second packet (from Computer A) was blocked from its destination (Computer B). See, for example, Figure 11 through Figure 14. In particular, after the user invoked the drop-down menu of the LSM GUI to change the filter setting from "Permit + Notify" to "Block + Notify" and the settings were saved (see Figure 11), the packet-filtering device was reconfigured to block HTTP protected file access threat packets from continuing toward their destinations.
1h. responsive to a determination by the packet-filtering device that the second packet	The TippingPoint system performs responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria: preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet.

Claim 1	Analysis of TippingPoint
corresponds to the one or more criteria: preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;	As described above in the analysis of claim elements 1a, 1b, and 1g, the second packet (from Computer A) was blocked from its destination (Computer B). See, for example, Figure 11 through Figure 14. In particular, after the 0361 filter was set to "Block + Notify" (see Figure 11), the second packet (from Computer A) was blocked from continuing toward its destination (Computer B).
1i. communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	The TippingPoint system performs communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet. As described above in the analysis of claim elements 1a, 1b, 1f, 1g, and 1h, the second packet was blocked. Furthermore, as shown in Figure 13, the Block Log of the LSM GUI indicates that the second packet was blocked. For the TippingPoint LSM GUI to display this log information to the user, the packet-filtering device must have communicated that the packet was blocked, communicating it to a data store served by the web server running on the TippingPoint IPS management interface. It is this web server that serves the content that is viewable by a user running the LSM GUI (which includes a web client connected to the web server running on the management interface).
1j. causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.	The TippingPoint system performs causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet. As described above in the analysis of claim elements 1a, 1b, 1f, 1g, and 1h, the second packet was blocked. Furthermore, as shown in Figure 13, the Block Log of the LSM GUI indicates that the second packet was blocked. This Block Log is a display in the LSM GUI that indicates that the second packet was prevented from continuing toward its destination.

Claim 25 Analysis

Claim 25	Analysis of TippingPoint
25. The method of Claim 1, wherein: receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices.	The TippingPoint system performs the method of Claim 1, wherein: receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices. As Figure 1 shows, TippingPoint IPS (specifically, the UnityOne-200 model) supports two different "segments" named SEG1 and SEG2. The prior testing supporting the Claim 1 analysis only made use of the SEG1 Ethernet ports (SEG1-A and SEG1-B). The SEG2 Ethernet ports (SEG2-A and SEG2-B) are inputs/outputs for a second packet-filtering device (in addition to the first packet filter on SEG1). The packet-filtering devices connected to SEG1 and SEG2 are two different packet-filtering devices. A diagram of the test network used for this analysis is shown in Figure 15.  **Figure 15: Network map for the test network used in the analysis of Claim 25.** The hardware comprising the test network used in this analysis is shown in Figure 16.

Claim 25	Analysis of TippingPoint

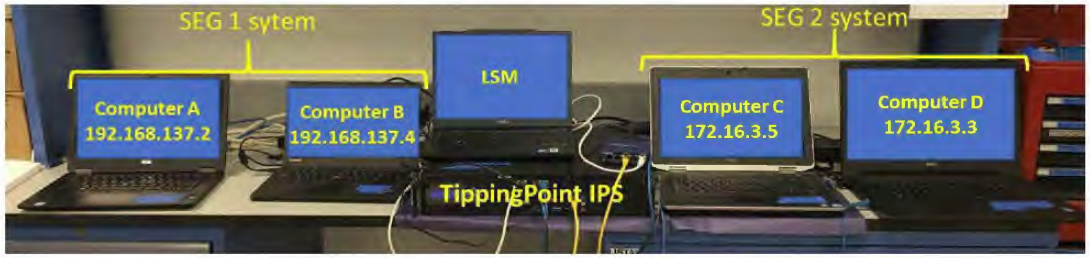


Figure 16: Annotated photograph of the test network used in Claim 25 analysis.

In addition, Figure 4 shows a variety of different packet-filtering rules that can be applied separately to either SEG1 or SEG2.

The TippingPoint IPS LSM allows independent operation of filters for each of the two segments. As an example, we set both filters to "Permit + Notify" for all. If both segments are set to "Permit + Notify," the packets are allowed through the system while being entered into the Alert Log, as shown in Figure 17. In the first line of the Alert Log, Computer B (192.168.137.4) sent an HTTP GET request for the URL path "/etc/passwd" on Computer A (192.168.137.2). In the second line of the Block Log, Computer D (172.16.3.3) sent an HTTP GET request for the URL path "/etc/passwd" on Computer C (172.16.3.5).

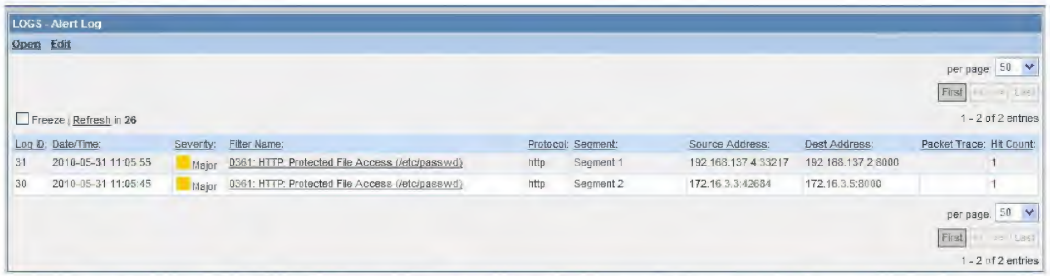


Figure 17: Screenshot from LSM GUI showing the Alert Log. Note that the upper log entry is for Segment 1 and the lower log entry is for Segment 2.

Claim 25	Analysis of TippingPoint
	If both segments are set to "Block + Notify," the packets are blocked by the system, and the incidents are entered into the "Block Log," as shown in Figure 18. In the first line of the Block Log, Computer B (192.168.137.4) sent an HTTP GET request for the URL path "/etc/passwd" on Computer A (192.168.137.2). In the second line of the Block Log, Computer D (172.16.3.3) sent an HTTP GET request for the URL path "/etc/passwd" on Computer C (172.16.3.5).

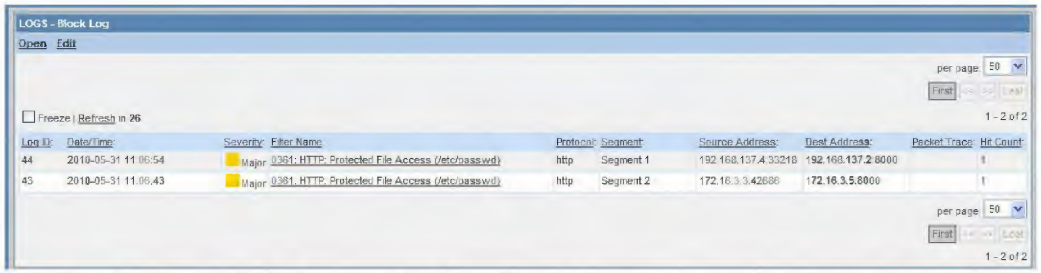


Figure 18: Screenshot from LSM GUI showing the Block Log. Note that the upper log entry is for Segment 1 and the lower log entry is for Segment 2.

Filter commands can be independently assigned to each of the two segments. This allows for independent operation of two packet-filtering devices. As an example, illustrated in Figure 19, we set all SEG1 filters to "Block + Notify" and all SEG2 filters to "Permit + Notify."

Claim 25	Analysis of TippingPoint



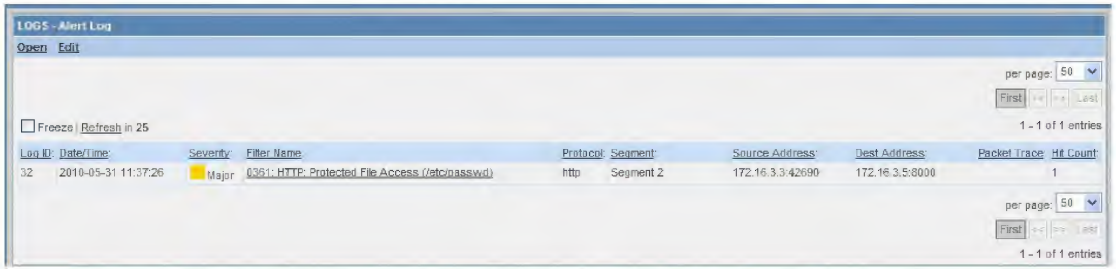
Figure 19: Screenshot from LSM GUI showing "Block + Notify" settings for Segment 1 and "Permit + Notify" settings for Segment 2.[13]

If these segment-specific filters are applied, then the threat packets sent through SEG1 are blocked (e.g., an HTTP GET request for the URL path "/etc/passwd" sent from Computer B to Computer A; see Figure 20) and threat packets sent through SEG2 are allowed (e.g., an HTTP GET request for the URL path "/etc/passwd" sent from Computer D to Computer C; see Figure 21).



Figure 20: Screenshot from LSM GUI showing that the HTTP: Protected File Access threat packet from Computer B (192.168.137.4) to Computer B (192.168.137.2) was blocked on Segment 1.

[13] Except "Performance Protection: Misuse and Abuse," which doesn't allow the "Permit + Notify" option.

Claim 25	Analysis of TippingPoint
	 **Figure 21: Screenshot from LSM GUI showing that the HTTP: Protected File Access threat packet from Computer D (172.16.3.3) to Computer C (172.16.3.5) was allowed on Segment 2.**

APPENDIX E

'722 Patent Analysis

Check Point R77

Contents

Claim 1 Analysis 1
Claim 25 Analysis 25

CENTRIPETAL-CSCO 087962

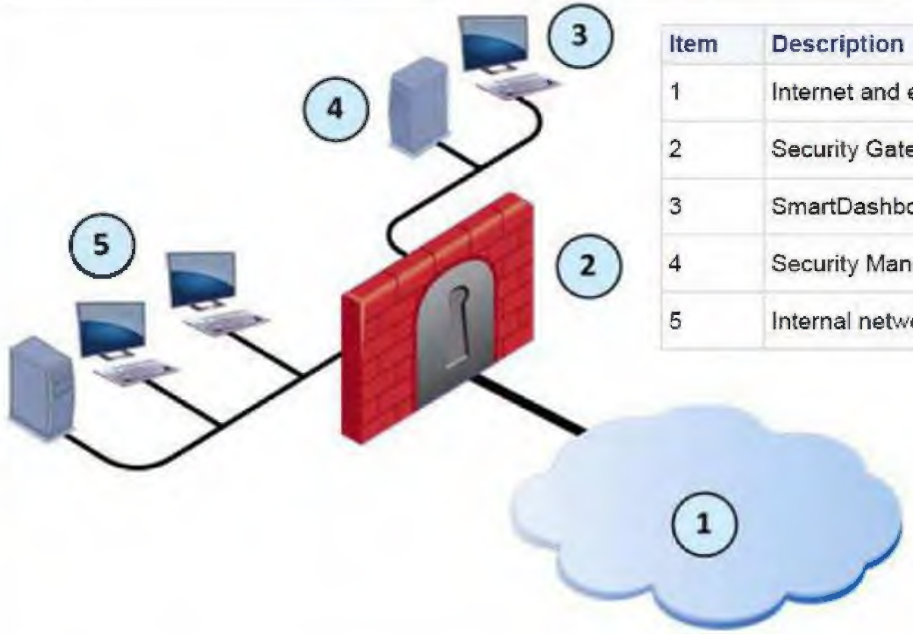
Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 462

Claim 1 Analysis

Claim 1	Analysis of Check Point R77
1a. A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;	The Check Point R77 is commercial software product comprising a security management server (SMS) program,[1] which when installed on suitable hardware constitutes a security policy management server, and a security gateway (SG) program,[2] which when installed on suitable hardware constitutes of a packet security gateway. Figure 1 illustrates how the Check Point R77 SG and R77 SMS fit into a typical network architecture. Exponent assembled and tested a network configured in this arrangement,wherein the components labeled "SMS" and "SG" in Figure 2 collectively form "the Check Point R77 system." As arranged in this test configuration, the Check Point R77 system performs a method comprising receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators.

[1] See "Check Point R77 Security Management Server Administration Guide" (dated Aug 27, 2013).
[2] See "Check Point R77 Firewall Administration Guide" (dated Aug 27, 2013).

Claim 1	Analysis of Check Point R77



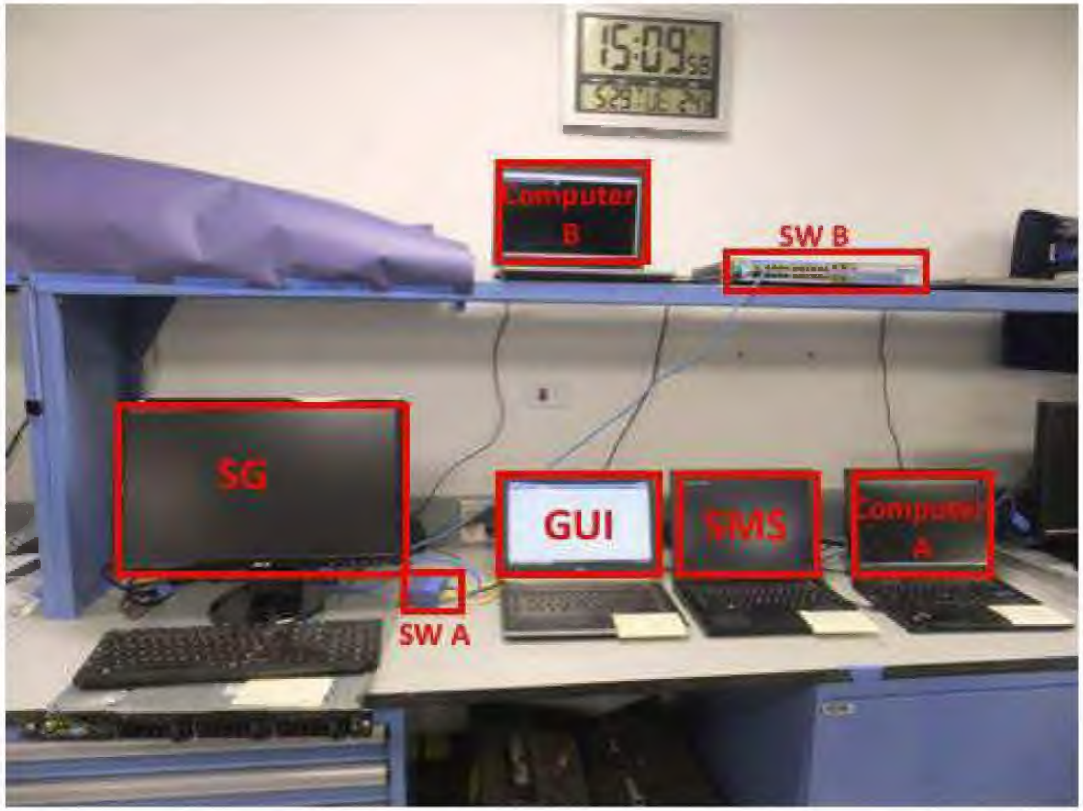
Item	Description
1	Internet and external networks
2	Security Gateway
3	SmartDashboard
4	Security Management Server
5	Internal network

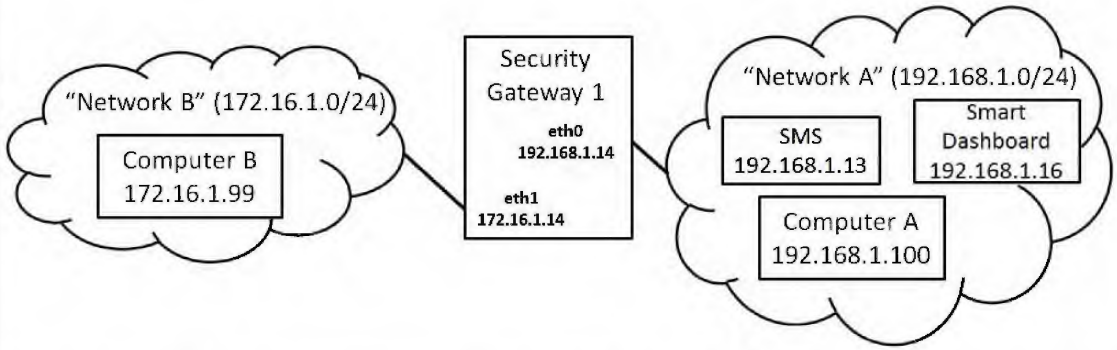
Figure 1: Typical deployment of a security gateway and a security management server (configurable using the SmartDashboard graphical user interface, or GUI). [3]

Exponent installed the Check Point R77 SMS product on a 32-bit PC-compatible Dell Latitude E6400 computer using the "Check_Point_R77.20_T124_Install.Gaia.iso" DVD ISO image (see "SMS" in Figure 2).

The Check Point R77 SG product was also installed on a 32-bit PC-compatible Dell PowerEdge 1750 computer (see "SG" in Figure 2).

[3] See pp. 9–10 CP_R77_Firewall_AdminGuide.

Claim 1	Analysis of Check Point R77
	Figure 2 shows the physical layout of the hardware, including the one security gateway, the security management server, the SmartDashboard (GUI), two switches (SW A and SW B), and two computers for sending and receiving packet traffic.  **Figure 2: Photograph of test network used as part of the claim analysis that shows a hardware installation of one security gateway and one security management server with its associated SmartDashboard GUI. Computers A and B reside in two separate networks connected by the security gateway. Each network has one switch to route traffic.**

Claim 1	Analysis of Check Point R77
	Figure 3 shows the schematic layout of the test network used in the analysis of this claim. Network A includes the R77 SMS along with another computer, Computer A with IP address 192.168.1.100. Network B includes a different computer called Computer B with IP address 172.16.1.99. Security Gateway 1 (SG 1), or simply "SG" in Figure 2, includes a packet-filtering device and protects Network B from Network A. The first subnet is called Network A and includes IP addresses in the range from 192.168.1.0 through 192.168.1.255. Network traffic internal to Network A is communicated via a TRENDnet TE100-S5 switch (Switch A). The second subnet is called Network B and includes IP addresses in the range from 172.16.1.0 through 172.16.1.255. Network traffic internal to Network B is communicated via a VLAN on an HP ProCurve 2510-24 that uses the ProCurve Ethernet ports numbered 1–12 (Switch B).  **Figure 3: Schematic of test network architecture, including the static IP address of each element. Each network has its own subnet. SG 1 protects Network B from Network A. It has two Ethernet network interfaces (eth0 and eth1), which are used to pass traffic between networks.** The Check Point R77 system allows the user to send a variety of different packet-filtering rules to one or

Claim 1	Analysis of Check Point R77
	more different packet-filtering devices. In the Check Point R77 system, these rules are configured and deployed by creating "security policies" and installing those policies on selected security gateways.[4] The policies that are installed on the gateway may correspond to specific network threats.[5] The SmartDashboard was used to install a policy that logs WebDAV HTTP methods. The policy can be configured either to allow offending packets to continue to their destination (by setting the policy action to "Detect") or to prevent offending packets from continuing to their destination (by setting the policy action to "Prevent"). Because WebDAV HTTP methods are not commonly used in conventional web browsing, the use of methods such as the WebDAV method "MKCOL" is considered a network threat. For example, the WebDAV HTTP request "MKCOL / HTTP/1.0" attempts to create a new directory, which is an uncommon request during normal web browsing. A packet containing such a request can be flagged as corresponding to a network threat and the associated packets can be logged and blocked. In the Check Point R77 test setup, SG 1 serves as a packet-filtering device and can be configured to identify packets based on packet-filtering rules, as shown in Figure 4. We configured specific HTTP method settings with the details shown in Figure 5 and installed on SG 1 to demonstrate that it can receive the packet-filtering rules, as shown in Figure 6 and Figure 7.

[4] See, generally, "CP_R77_SecurityManagement_AdminGuide.pdf" (dated 27 August 2013) and "CP_R77_Firewall_AdminGuide.pdf" (dated 27 August 2013).

[5] See "CP_R77_Firewall_AdminGuide.pdf" (dated 27 August 2013) at Chapters 7 and 8.

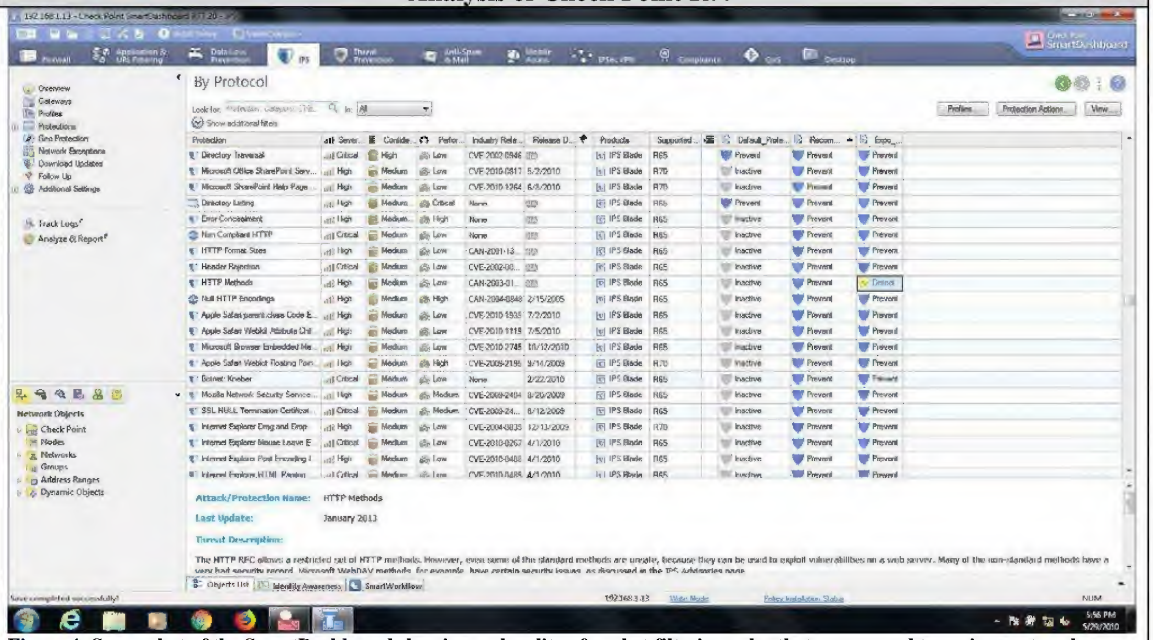
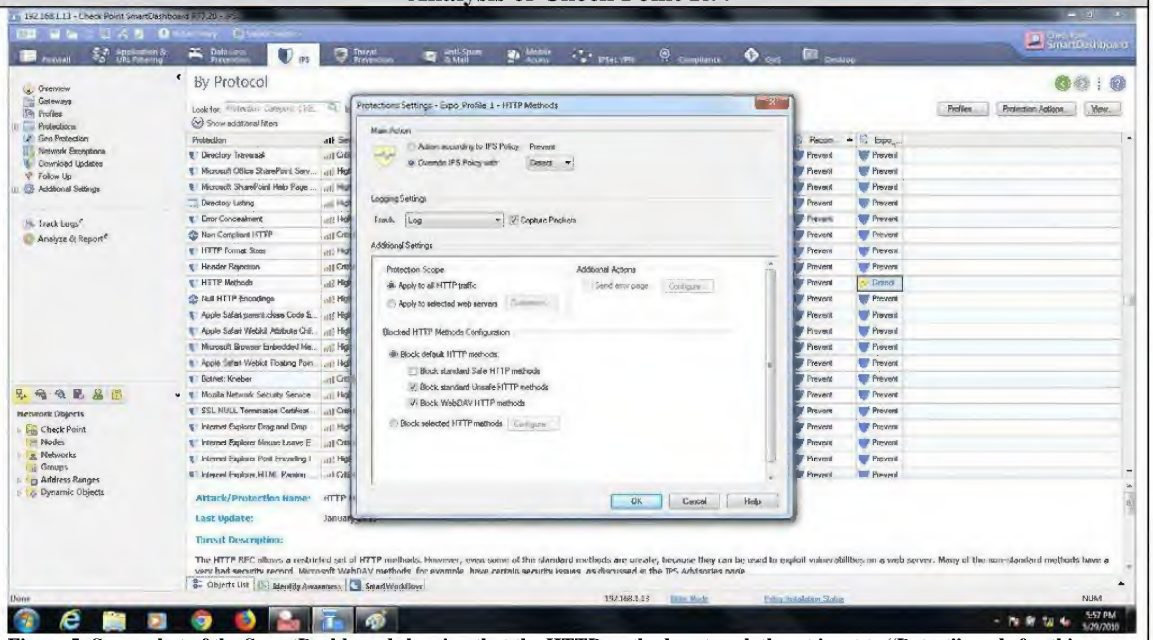
Claim 1	Analysis of Check Point R77
	

Figure 4: Screenshot of the SmartDashboard showing a plurality of packet-filtering rules that correspond to various network threats.

CENTRIPETAL-CSCO 087968

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 468

Claim 1	Analysis of Check Point R77
	 **Figure 5: Screenshot of the SmartDashboard showing that the HTTP methods network threat is set to "Detect" mode for this policy.**

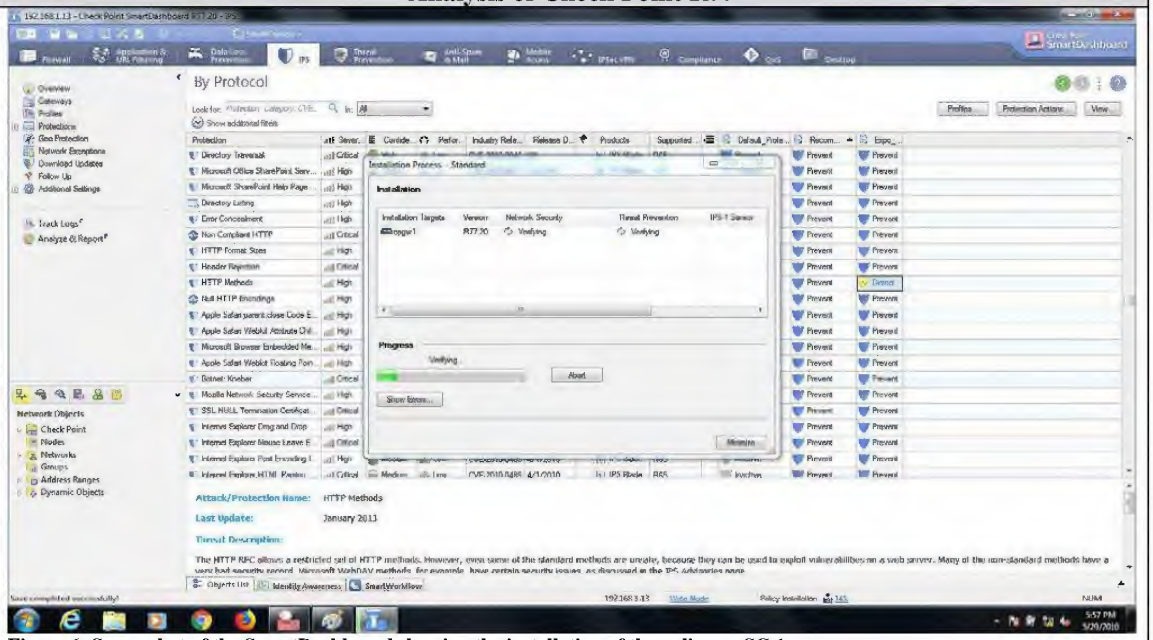
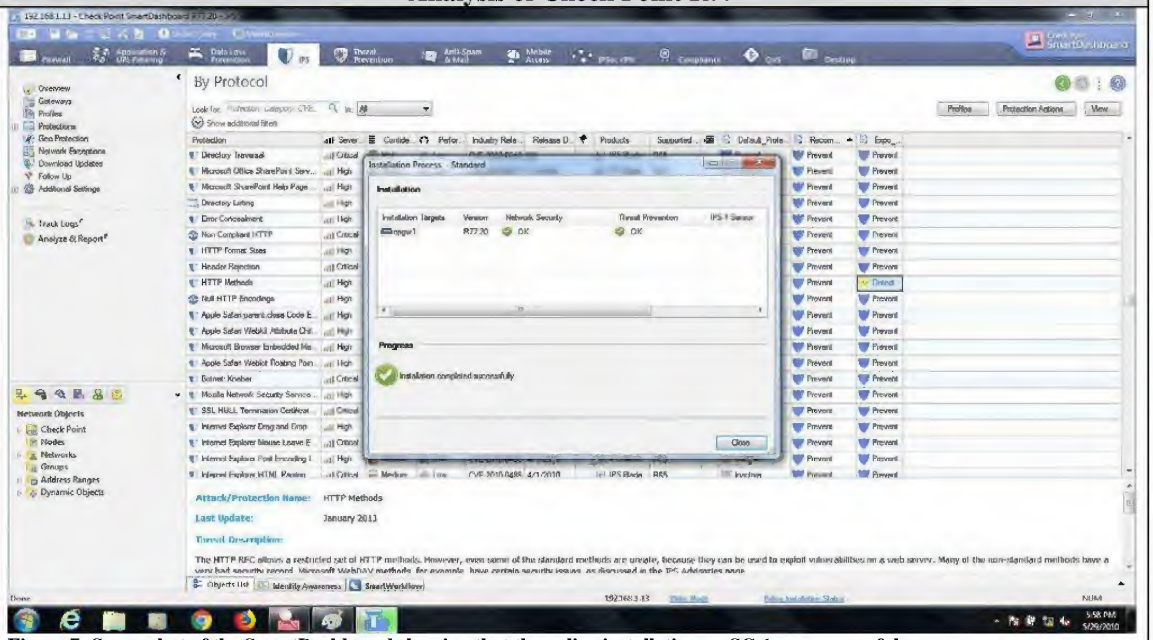
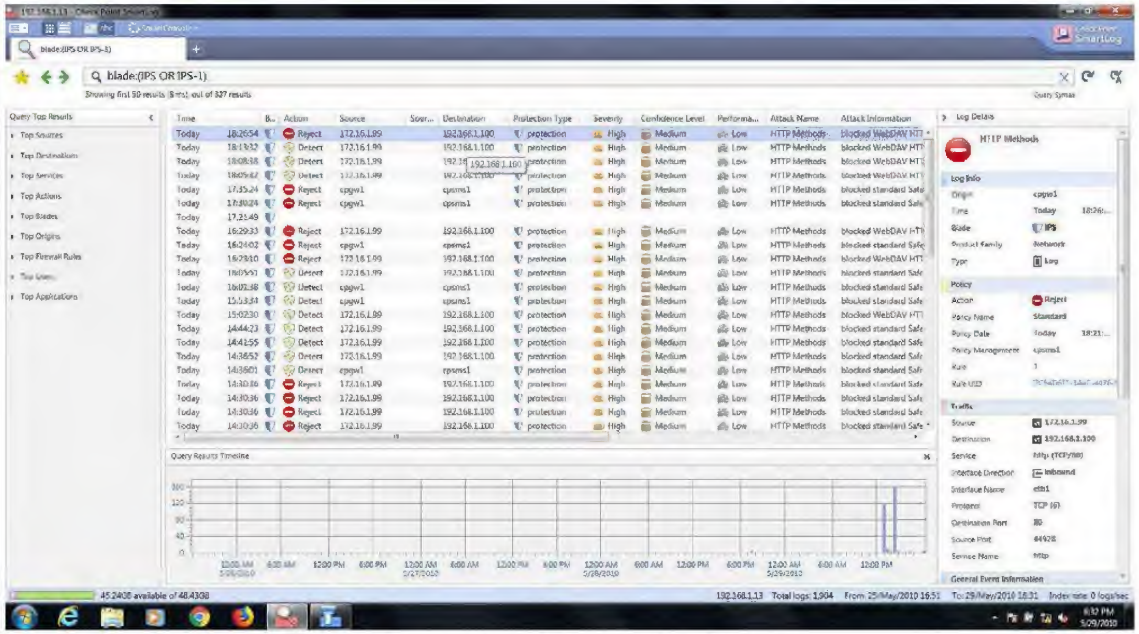
Claim 1	Analysis of Check Point R77
	

Figure 6: Screenshot of the SmartDashboard showing the installation of the policy on SG 1.

CENTRIPETAL-CSCO 087970

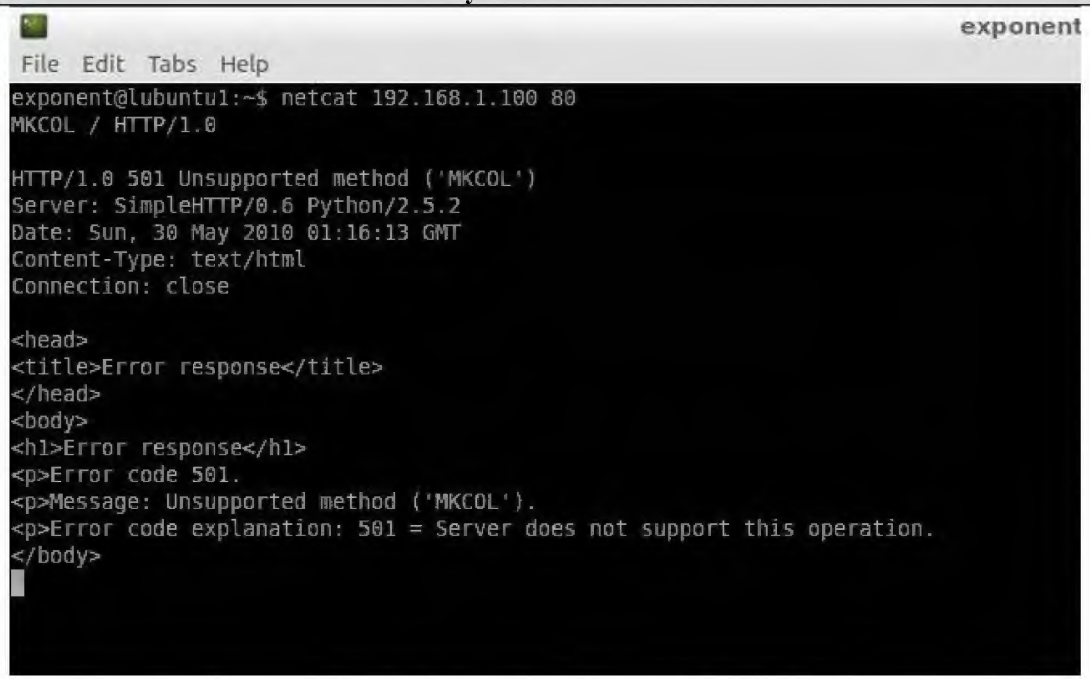
Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 470

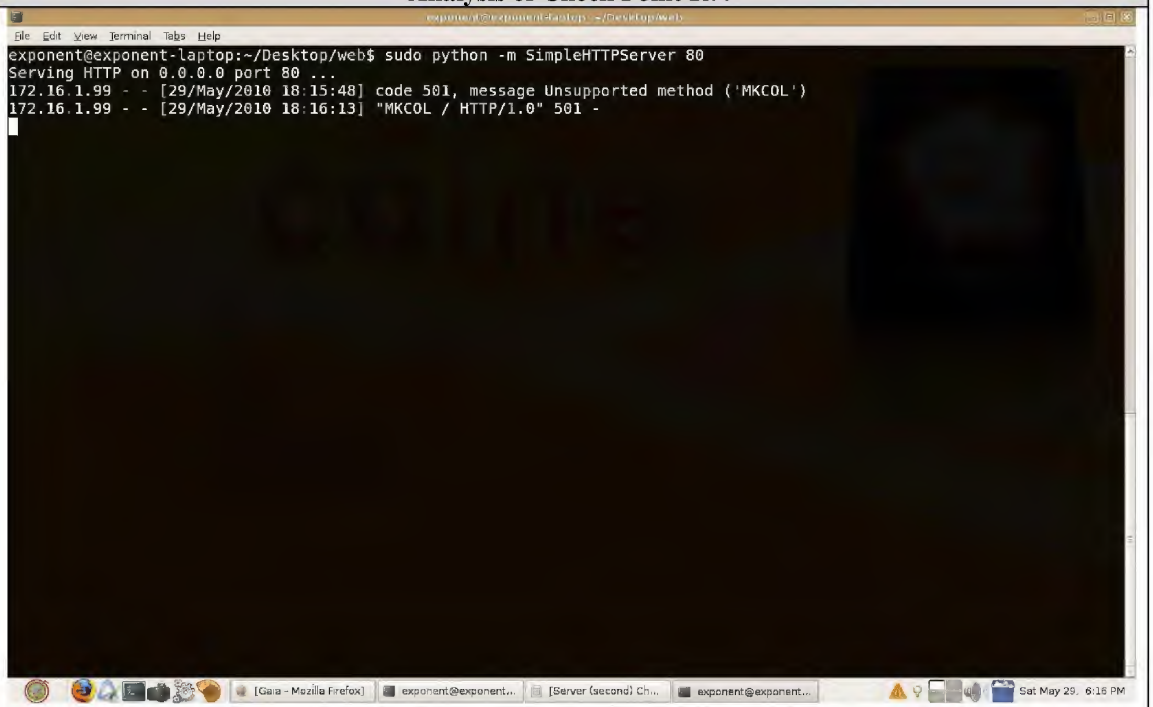
Claim 1	Analysis of Check Point R77
	 **Figure 7: Screenshot of the SmartDashboard showing that the policy installation on SG 1 was successful.** Thus, the testing has demonstrated that the packet filtering device of the Check Point R77 system recieves a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators.
1b. receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second	The tested Check Point R77 system performs a method comprising: receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet. The Check Point R77 includes a SmartLog program to log the action of the packets that are received by the SG. Figure 8 shows that the SG receives a plurality of packets, including a first packet, a second

Claim 1	Analysis of Check Point R77
packet;	packet, and more. In this case, both the first packet and the second packet correspond to the HTTP methods network threat described in claim element 1a.  **Figure 8: Screenshot of the SmartLog showing a plurality of packets having been received.** Thus, the testing has demonstrated the packet-filtering device of the Check Point R77 system receives a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet.
1c.responsive to a determination by the packet-filtering device that the first packet satisfies	The tested Check Point R77 system performs a method comprising: responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators: applying, by the packet-filtering device and to the first packet,

Claim 1	Analysis of Check Point R77
one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators: applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet;	an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet. A packet-filtering rule corresponding to the HTTP methods network threat (which filters uncommon WebDAV HTTP requests) was previously installed on the SG. See analysis of claim element 1a. An HTTP request (including a first packet) was sent from Computer B to Computer A. Figure 9 illustrates this request, which shows: (1) the initiation of a connection from Computer B to Computer A using the "netcat" utility (first line), (2) the HTTP request "MKCOL / HTTP/1.0" including the MKCOL method (second line), and (3) the response received from Computer A (remaining lines). Of note, the response from Computer A is a 501 error code, indicating that the HTTP server[6] does not support the MKCOL method (along with some response headers and some HTML code indicating the error). This means that the packet sent from Computer B was allowed to pass through the packet filter to Computer A, which received the packet and sent back the error code. Additionally, Figure 10 shows the terminal session from HTTP server on Computer A. This figure displays the received MKCOL HTTP request on the fourth line.

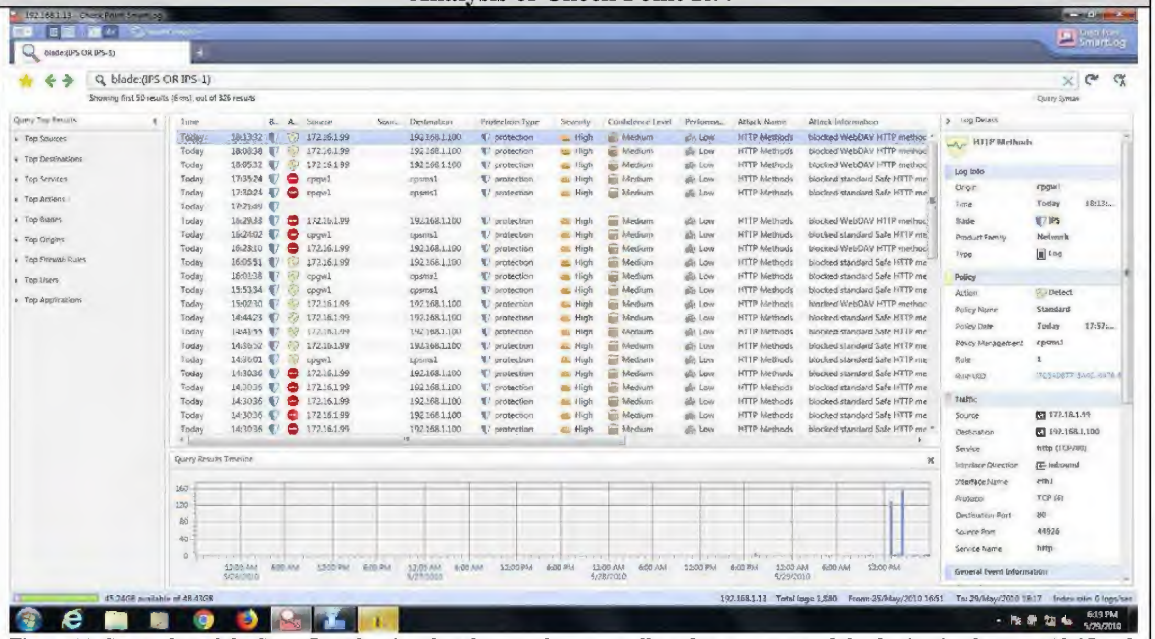
[6] The HTTP server being used is the python SimpleHTTPServer module. For more information, see https://docs.python.org/2/library/simplehttpserver.html.

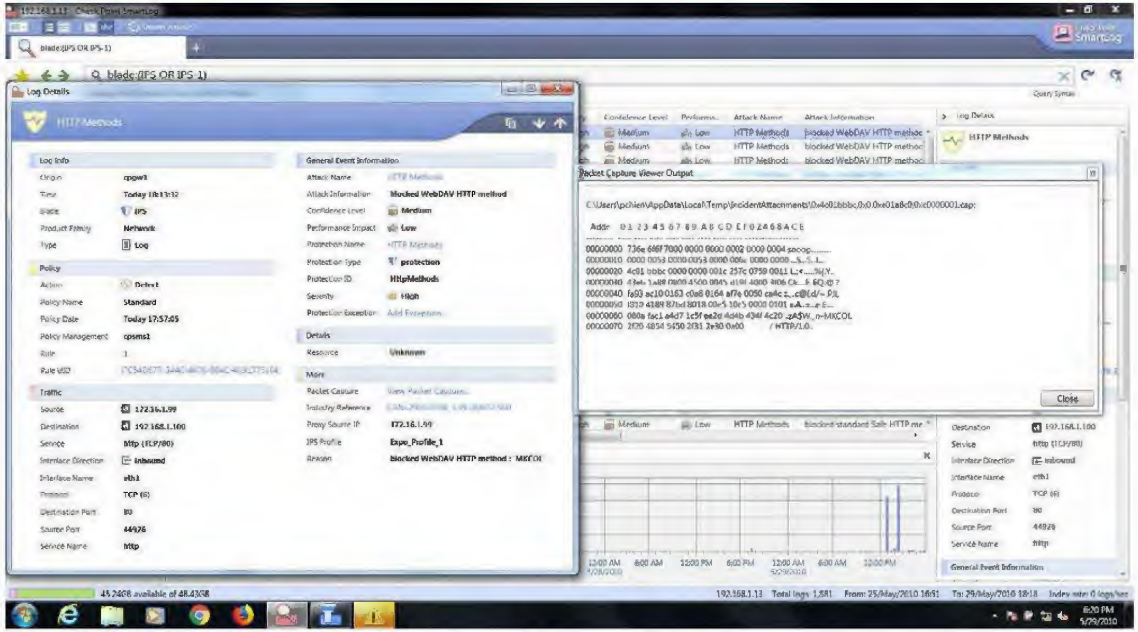
Claim 1	Analysis of Check Point R77
	 **Figure 9: Screenshot of Computer B illustrating the connection to Computer A (192.168.1.100) and successful send of the first packet.**

Claim 1	Analysis of Check Point R77
	 **Figure 10: Screenshot of Computer A showing the successful receipt of the first packet from Computer B (172.16.1.99).** Thus, the testing has demonstrated that the packet-filtering device of the Check Point R77 system applies an operator (specified by the packet-filtering rule that is configured to cause the packet-filtering device to allow the first packet to continue toward its destination) to the first packet. This operator selection according to the packet-filtering rule is made in response to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules that correspond to one or more network-threat indicators of the plurality of network-threat indicators.

Claim 1	Analysis of Check Point R77
1d. communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;	The tested Check Point R77 system performs communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet. The packet-filtering device (SG 1) communicates with the SMS that the first packet was allowed to pass, as shown in the SmartLog contained in Figure 11. The source of the first packet is 172.16.1.99 (Computer B), and the destination of the packet is 192.168.1.100 (Computer A). The specific network-threat that is being evaluated by the packet-filtering device is the HTTP Methods threat, as indicated in the "Attack Name" column shown in Figure 11. The Check Point R77 SmartLog program[7] displays log files stored on the computer hosting the SMS. In order for the SmartLog program to display the information that the network attack packet corresponding to the HTTP methods threat was allowed, SG 1 must have communicated (to the SMS) data indicative that the packet was allowed.

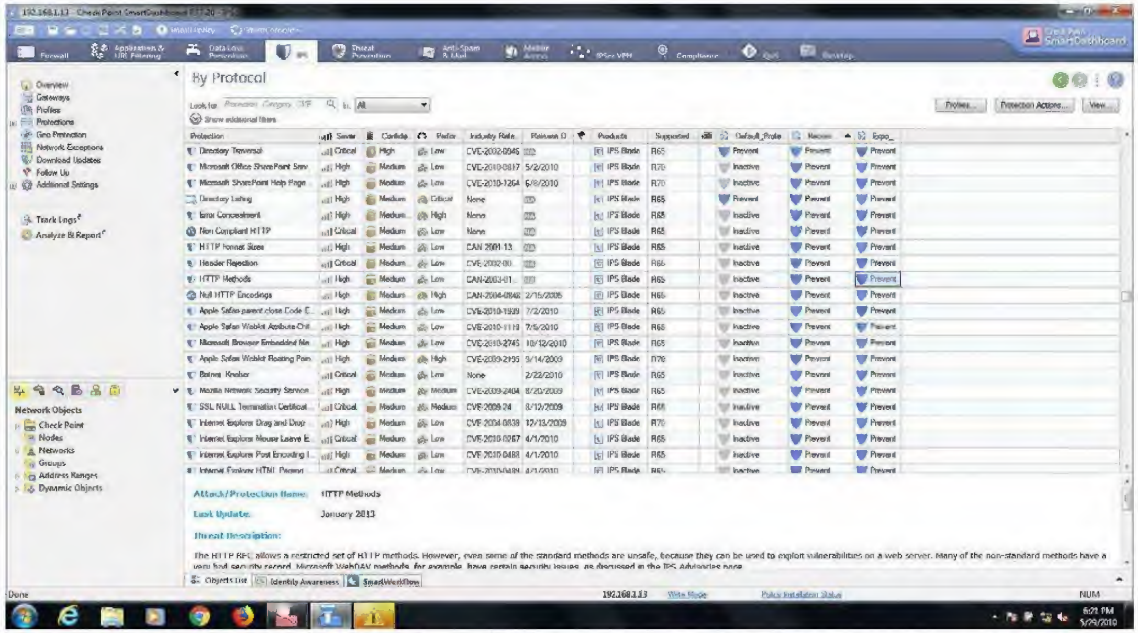
[7] See, generally, "CP_R77_SmartLog_AdminGuide.pdf" (dated 26 August 2013).

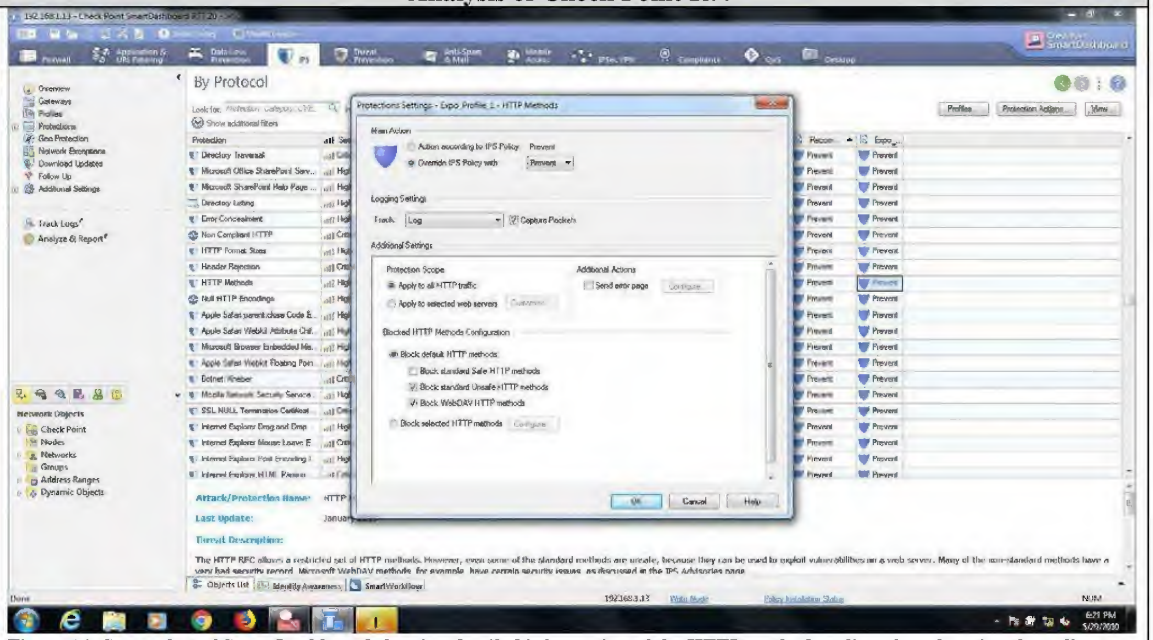
Claim 1	Analysis of Check Point R77
	 **Figure 11: Screenshot of the SmartLog showing that three packets were allowed to move toward the destination between 18:05 and 18:13 on the system clock. The 3rd column from the left in the table (with heading "A...") corresponds to the action taken, and the yellow shield symbol in the first three rows of this column indicates that the packet was allowed to pass from Computer B (172.16.1.99) to Computer A (192.168.1.100).** Thus, the testing has demonstrated that the packet filtering device of the Check Point R77 system communicates information from the packet-filtering rule that identifies the one or more network-threat indicators and data indicative that the first packet was allowed to continue toward the destination of the first packet.
1e. causing, by the packet-filtering device and in an interface, display of the	The Check Point R77 system performs a method causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators.

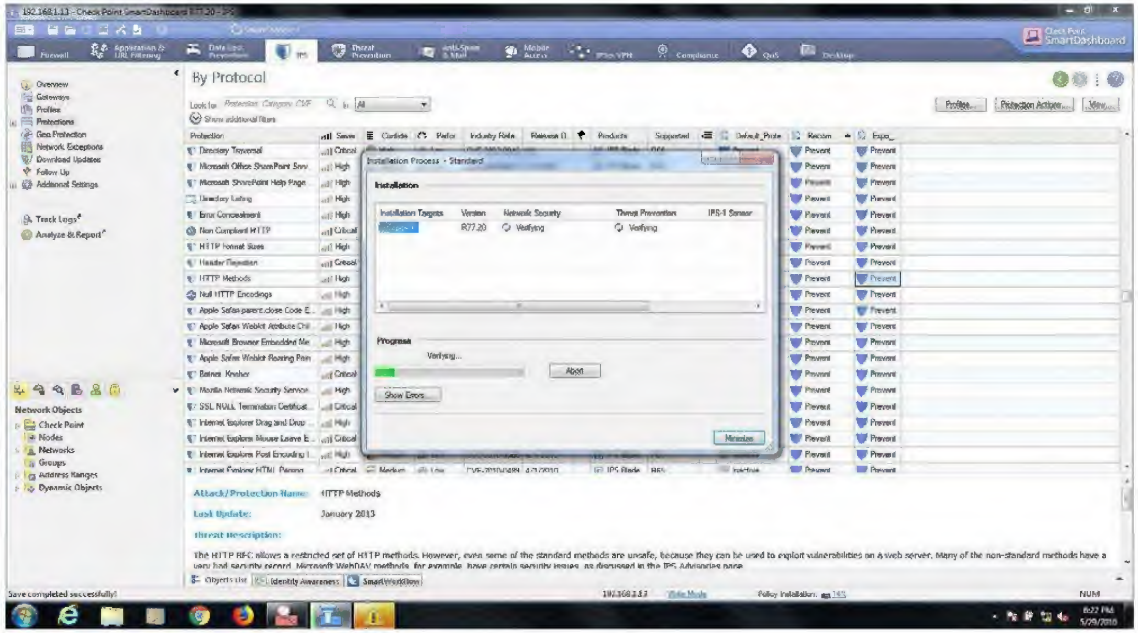
Claim 1	Analysis of Check Point R77
information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;	See analysis of claim element 1d, especially Figure 11 which shows that the packets were allowed to move toward their destination. See also Figure 12 which shows a GUI that displays information about the details of the packet-filtering rule for the HTTP methods network threat.  **Figure 12: Screenshot of the SmartLog showing the details of the packets allowed to move toward the destination.** Thus, the testing has demonstrated that the R77 Check Point system has an interface which, in at least one portion of said interface, displays information from the packet-filtering device corresponding to the packet-filtering rule and one or more network-threat indicators.
1f. receiving, by the	The Check Point R77 system performs a method receiving, by the packet-filtering device, an instruction

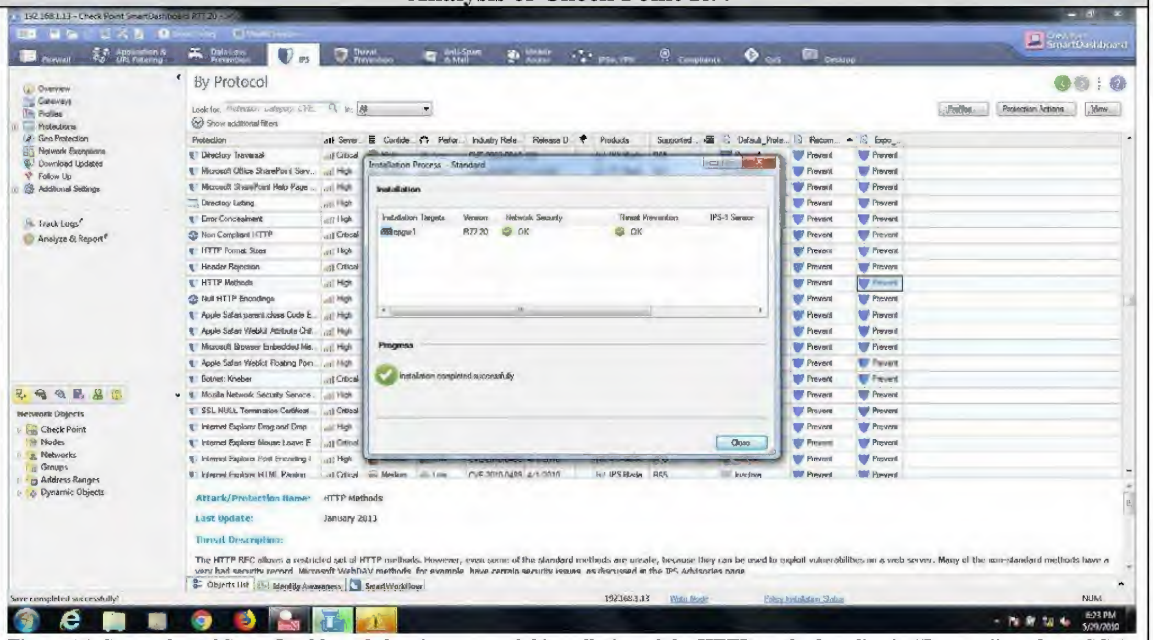
CENTRIPETAL-CSCO 087978

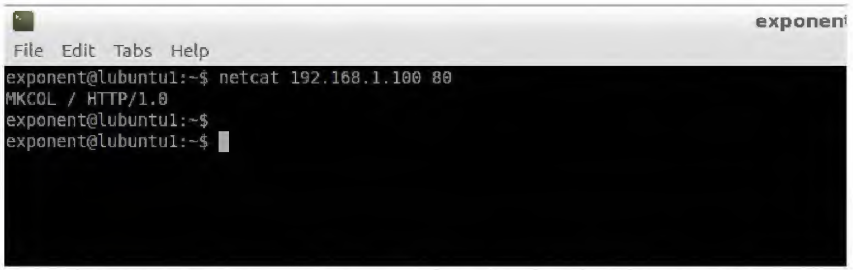
Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 478

Claim 1	Analysis of Check Point R77
packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and	generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators. The HTTP methods network attack settings were initially configured to detect the attack, as Figure 4 shows, but not block it. After the first packet was logged (detected), the user reconfigured the HTTP methods attack settings from "Detect" to "Prevent" by clicking near the highlighted section in the right-most column of the table contained in the SmartDashboard GUI shown Figure 13. The updated policy was then installed on the security gateway. The updated settings are also shown in Figure 14.  **Figure 13: Screenshot of SmartDashboard showing the HTTP methods policy in "Prevent" mode. This change was in response to user action.**

Claim 1	Analysis of Check Point R77
	 **Figure 14: Screenshot of SmartDashboard showing detailed information of the HTTP methods policy after changing the policy to "Prevent."** Thus, the testing has demonstrated that the packet-filtering device receives an instruction generated in response to a user invoking an element in at least one portion of the interface corresponding to the packet-filtering rule and one or more network-threat indicators.
1g. responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the	The Check Point R77 system performs a method responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations.

Claim 1	Analysis of Check Point R77
packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and	The packet-filtering rule corresponding to the HTTP methods network attack was installed on SG 1, as shown in Figure 15 and Figure 16. Thus, SG 1 was reconfigured to block this attack—that is, to block packets containing WebDAV HTTP methods from continuing toward their respective destinations.  **Figure 15: Screenshot of SmartDashboard showing the installation of policies on SG 1.**

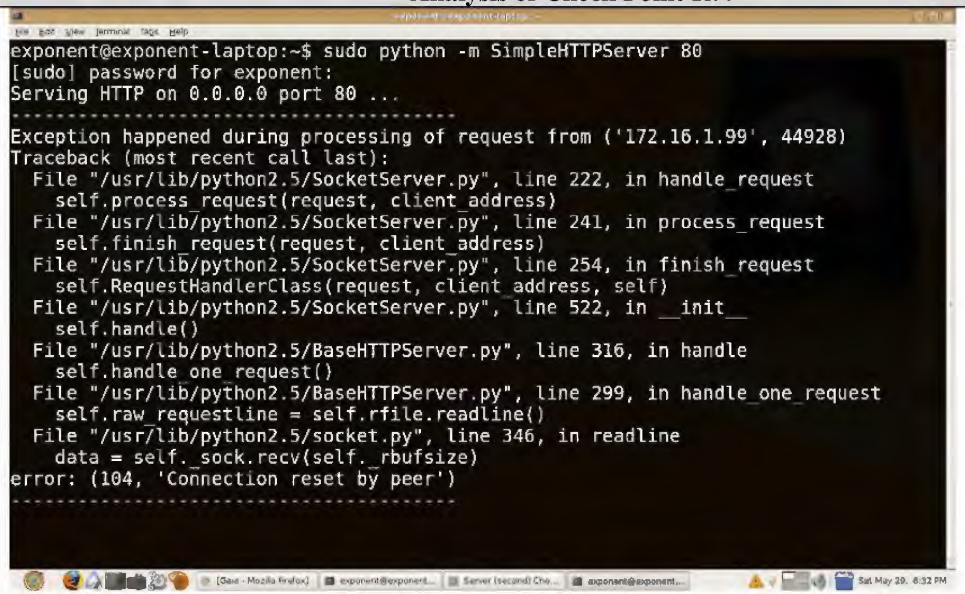
Claim 1	Analysis of Check Point R77
	 **Figure 16: Screenshot of SmartDashboard showing successful installation of the HTTP methods policy in "Prevent" mode on SG 1.** Thus, the testing has demonstrated that in response to receiving the instruction, the packet-filtering device modifies at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to one or more criteria from continuing toward their respective destinations.
1h. responsive to a determination by the packet-filtering device that the second packet corresponds to the one or	The Check Point R77 system performs a method responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria: preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet; A security policy containing a packet-filtering rule corresponding to the HTTP methods threat was

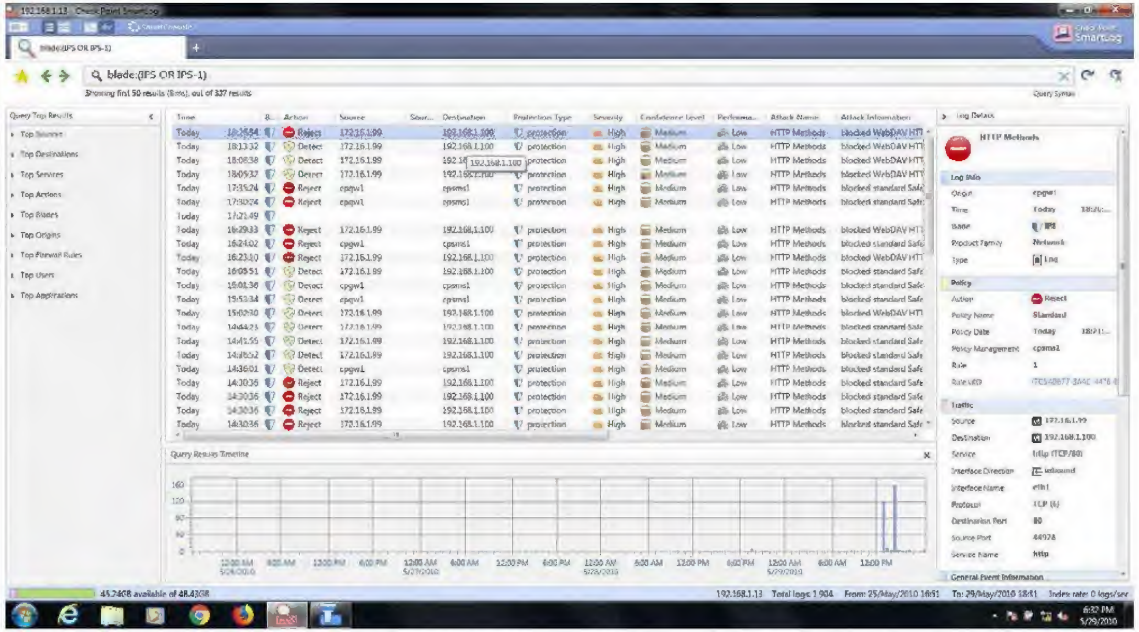
Claim 1	Analysis of Check Point R77
more criteria: preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;	previously installed on SG 1. See analysis of claim element 1g. A WebDAV HTTP request including the second packet was sent from Computer B to Computer A. Figure 9 illustrates this action and shows: (1) the initiation of a connection from Computer B to Computer A using the netcat utility (first line), (2) the HTTP request "MKCOL / HTTP/1.0" including the MKCOL method (second line), and (3) the lack of a response (no subsequent lines of the netcat session). Because the second packet was prevented from continuing toward its destination, Computer A never received the HTTP request from Computer B. Therefore, Computer B did not send back a response. Had Computer B received the HTTP request, it would have sent back a response, including a 501 error code. Thus, the second packet was prevented from continuing toward its destination. Furthermore, Figure 18, which depicts the terminal session from the HTTP server running on Computer A, shows that the server did not receive a MKCOL request.[8]  **Figure 17: Screenshot of Computer B unsuccessfully sending the WebDAV request to Computer A.**

[8] Rather, the connection was dropped leading to the cascade of exceptions shown in the lower half of the figure.

CENTRIPETAL-CSCO 087983

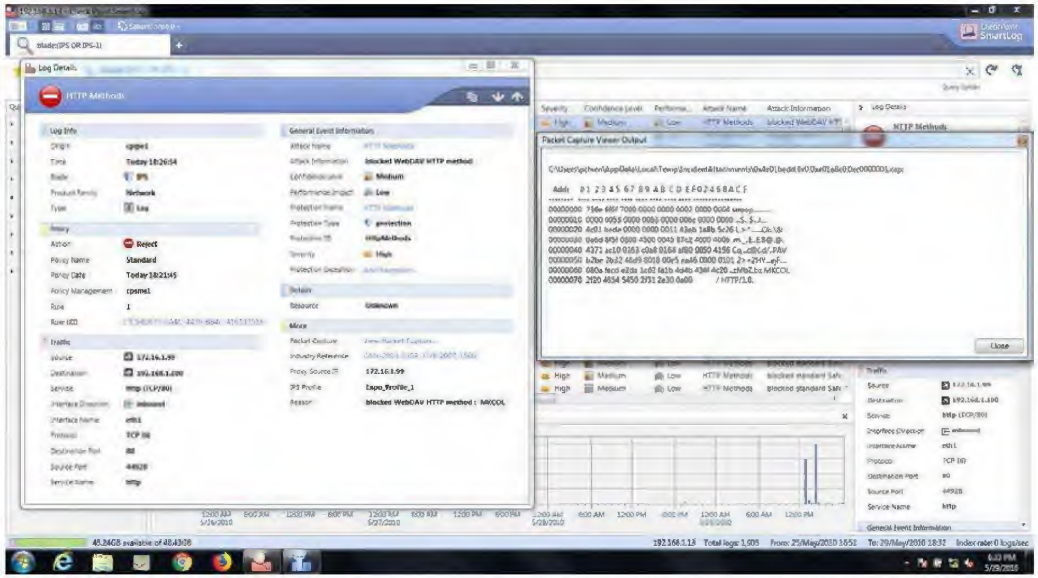
Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 483

Claim 1	Analysis of Check Point R77
	 **Figure 18: Screenshot of Computer A showing that the packet-filtering device prevented the WebDAV request from Computer B.** Thus, the testing has demonstrated that, in response to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria that was modified in claim element 1g, the packet-filtering device prevents the second packet from continuing toward a destination of the second packet.
1i. communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of	The Check Point R77 system performs a method which communicates, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet. The Check Point SmartLog shows data indicative that the second packet was prevented from moving toward its intended destination. As Figure 19 shows, the SmartLog indicates that the HTTP method

Claim 1	Analysis of Check Point R77
the second packet; and	network threat was rejected by the packet-filtering device and was thereby prevented from continuing toward its intended destination. In order for the SmartLog program to display the information that the network attack packet corresponding to the HTTP methods threat was blocked, SG 1 must have communicated data to the SMS to indicate that the packet was blocked.  **Figure 19: Screenshot of the SmartLog showing a packet was prevented from moving toward the destination. Only the top event listed in the log (corresponding to a system time of 18:26:54) corresponds to a packet that was sent after the change in HTTP Methods protections setting to "Prevent" shown in Figure 16. The prior events that were logged on or before system time 18:13:32 occurred when the HTTP Methods protections was set to "Detect" (see Figure 11).** Thus, the testing has demonstrated that the packet-filtering device communicates data which indicates that the second packet was prevented from continuing toward its intended destination.

CENTRIPETAL-CSCO 087985

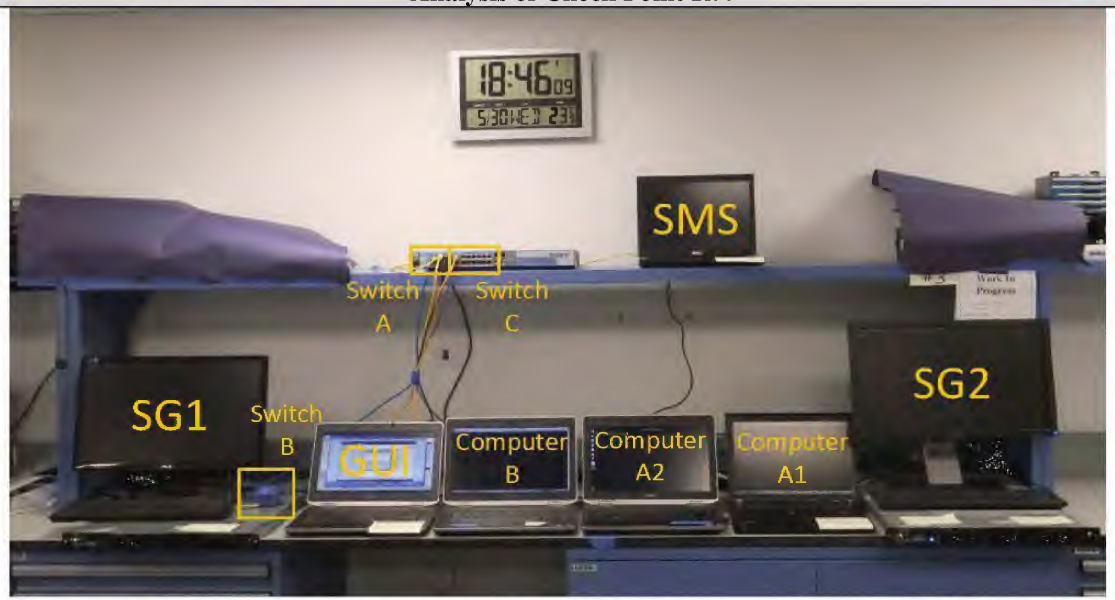
Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 485

Claim 1	Analysis of Check Point R77
1j. causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.	The Check Point R77 system performs a method causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet. The analysis of claim element 1i, especially Figure 19, shows that the packet-filtering device (SG 1) must have communicated that the second packet was prevented from passing to its intended destination . Furter, Figure 20 shows a GUI that displays information about the details of the packet-filtering rule for the HTTP methods network threat as claimed by element 1j. The SmartLog displays details indicating that the second packet was prevented from moving toward its intended destination.  **Figure 20: Screenshot of the SmartLog showing details of the packets prevented from moving toward the destination.**

Claim 1	Analysis of Check Point R77
	Thus, the testing has demonstrated the interface of the packet-filtering device displays data indicating that the second packet was prevented from continuing toward its destination.

Claim 25 Analysis

Claim 25	Analysis of Check Point R77
25. The method of Claim 1, wherein: receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices.	The Check Point R77 system performs the method of Claim 1, wherein receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices. Figure 21 shows the physical hardware setup used to demonstrate that the Check Point R77 satisfies all requirements added to Claim 1 by Claim 25.

Claim 25	Analysis of Check Point R77
	 **Figure 21: Annotated photograph of the test network used as part of this and subsequent claim analyses. The figure shows a hardware installation including two security gateways (SG1 and SG2) and one security management server (SMS) with its associated SmartDashboard GUI. Computers A1 and A2 reside in Network A. Computer B resides in Network B. Networks A and B are connected by SG1.** Figure 22 shows the corresponding network map for the extended test network that includes two different security gateways, SG1 and SG2.

Claim 25	Analysis of Check Point R77

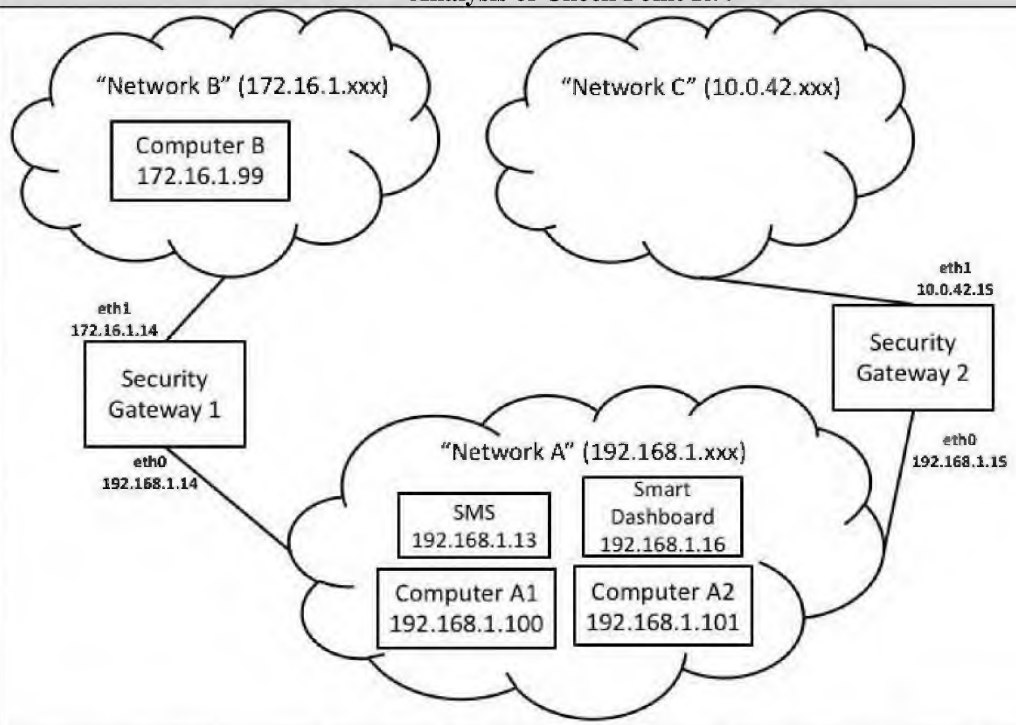
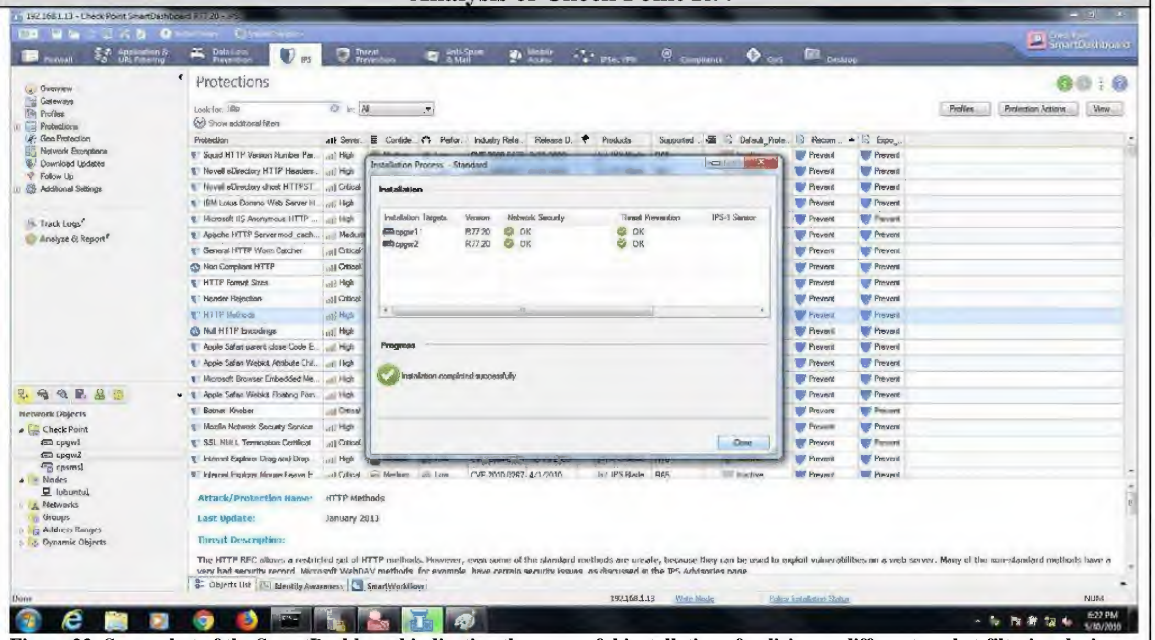


Figure 22: Schematic of test network architecture, including the static IP address of each element. Each network has its own subnet. Security Gateway 1 protects Network B from Network A. Security Gateway 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (eth0 and eth1), which are used to pass traffic between networks.

The packet-filtering device (SG 1) is connected to two networks via two separate Ethernet ports. The first packet-filtering device is connected to Network A via Switch A and is connected to Network B via Switch B, as Figure 21 shows. Figure 21 also shows a second packet-filtering device (SG 2). The first subnet is called Network A and includes IP addresses in the range from 192.168.1.0 through 192.168.1.255. Network traffic internal to Network A is communicated via a VLAN on an HP ProCurve 2510-24 that uses the ProCurve Ethernet ports 1–12 (Switch A). The second subnet is called Network B

Claim 25	Analysis of Check Point R77
	and includes IP addresses in the range from 172.16.1.0 through 172.16.1.255. Network traffic internal to Network B is communicated via a TRENDnet TE100-S5 switch (Switch B). The third subnet is called Network C and includes IP addresses in the range from 10.0.42.0 through 10.0.42.255. Network traffic internal to Network C is communicated via a VLAN on a HP ProCurve 2510-24 that uses the ProCurve Ethernet ports 13–24 (Switch C). For the analysis of this claim, Network B is taken as the first network and Network A is taken as the second network. For the analysis of this claim, the first host in the second network is taken to be Computer A2 and the second host in the second network is taken to be Computer A1. Both SG1 and SG2 can be independently configured via the Check Point R77 SMS GUI. The laptop labeled "SMS" in Figure 21 running the Check Point R77 SMS program constitutes "one or more computing devices" that, in the same way as demonstrated in relation to Claim 1 for Check Point R77 SG1, can "provide packet-filtering rules" to both SG1 and SG2. Multiple policies were installed via the computer running SmartDashboard on multiple packet-filtering devices (Security Gateway SG 1 "cpgw1" and Security Gateway SG 2 "cpgw2"), as shown in Figure 23. These policies contain multiple different packet-filtering rules, as indicated by the different protection categories contained in the 1st column on the left of the GUI table in Figure 23.

Claim 25	Analysis of Check Point R77
	 **Figure 23: Screenshot of the SmartDashboard indicating the successful installation of policies on different packet-filtering devices.** Thus, the testing has demonstrated the method of Claim 1, wherein receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices.

CENTRIPETAL-CSCO 087991

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 491

APPENDIX F

'213 Patent Analysis

TippingPoint IPS

Contents

Claim 1 analysis 3
Claim 3 analysis 25

CENTRIPETAL-CSCO 087993

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 493

Claim 1 analysis

Claim 1	Analysis TippingPoint IPS
1a. A method comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;	The TippingPoint UnityOne-200 Intrusion Prevention System (hereinafter, "TippingPoint IPS" or "TippingPoint system") performs a method, comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information. Exponent obtained a TippingPoint IPS device with part number SBASY-199 Rev: C03 and serial number ST05170004, as shown in Figure 1. As required by the patent, the TippingPoint system comprises two packet security gateways (SEG 1 and SEG 2) and one security policy management server (the local security manager, or LSM), as described further below.



Figure 1: TippingPoint IPS hardware showing the part number and serial number of the device.

The TippingPoint system includes a local security manager (LSM), which "is the control center from which you can configure, monitor, and report on the UnityOne Intrusion Prevention System (IPS) devices in your network."[1]

[1] "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. xi.



Figure 2: Annotated photographs of the TippingPoint IPS showing two packet security gateway interfaces (lower left) and one management interface (lower right).

The TippingPoint IPS includes two separate Ethernet port pairs called "segments," which act as two separate packet security gateways; each segment can be programmed to follow its own set of filtering rules via the LSM. As such, the LSM is a security policy management server which can provide rules, messages, instructions, etc. to the segment packet security gateways. Additional security policy management server functionality is performed in part via a web server running on the MGMT Ethernet interface of the TippingPoint IPS, indicated in the red annotations in Figure 2.

The TippingPoint IPS LSM "is a graphical user interface (GUI) that enables you to monitor and configure your UnityOne Intrusion Prevention System (IPS) using an ordinary web browser."[2] To access this GUI, an Ethernet cable was connected between the MGMT port of the IPS and a computer running Windows XP with Internet Explorer 7.[3]

An image of a TippingPoint IPS test setup is shown in Figure 3:

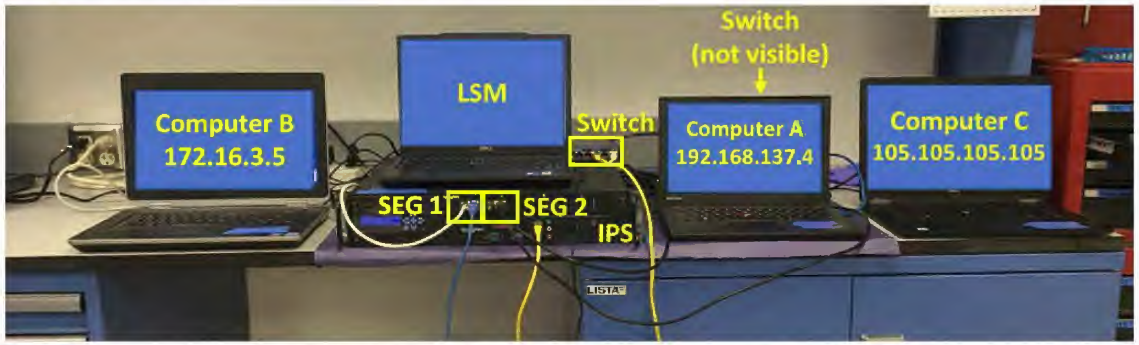


Figure 3: Image of test network used as part of the claim analysis that shows a hardware installation of one IPS containing a security management server and two packet security gateways ("SEG 1" and "SEG 2"). The laptop labeled "LSM" is used to connect to the LSM web server located on the TippingPoint IPS device. Computers A, B, and C reside in separate network address spaces and are connected by the two packet security gateways.

Figure 3 shows the physical layout of the hardware, including the IPS with its two packet security gateways (SEG 1 and SEG 2) and the security management server (located on-board the Tipping Point IPS device), the LSM interface laptop, two switches, and three additional laptop computers for sending and receiving packet traffic.

The test network shown in includes computers with IP addresses in three different network address spaces. Figure 4 shows the schematic layout of the test network.

---

2 "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 8.

3 The TippingPoint IPS web server was found to be incompatible with modern versions of Internet Explorer. Internet Explorer 7 was released circa 2006. (See, for example, https://en.wikipedia.org/wiki/Internet_Explorer_version_history#Windows_Internet_Explorer_7.)

	The first network is called "Network A" and includes IP addresses in the range from 192.168.1.37.2 through 192.168.137.5. Network traffic internal to Network A is communicated via a TP-Link TL-SG108 Switch (not visible in Figure 3). The second network is called "Network B" and includes a computer with IP address 172.16.3.5. Network A and Network B are connected by the first packet security gateway, which is the packet security gateway labeled SEG 1 in Figure 3. The test network shown in Figure 3 also includes a third network, called "Network C," that includes a computer with IP address 105.105.105.105. Network A and Network C are connected by the second packet security gateway, which is the packet security gateway labeled SEG 2 in Figure 3. In the test configuration, Network A includes Computer A. Network B includes Computer B. Network C includes Computer C. The first packet security gateway (SG1, associated with Segment 1, or SEG 1) protects Network B from Network A. The second packet security gateway (SG2, associated with Segment 2, or SEG 2) protects Network C from Network A.

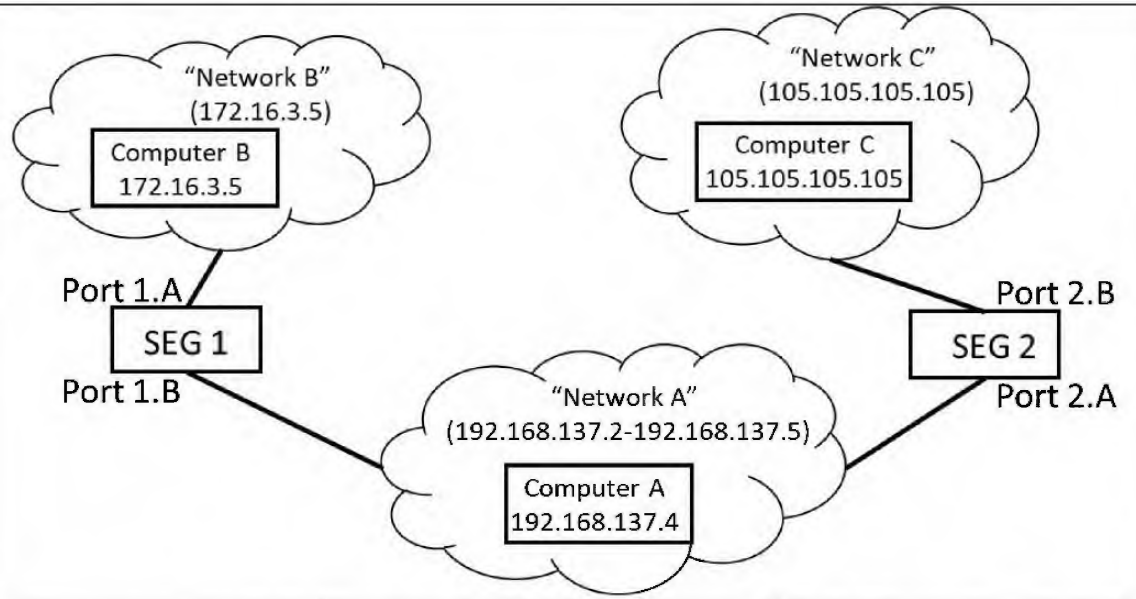


Figure 4: Schematic of the test network (see Figure 3) architecture, including the static IP addresses of each element. Each network has its own subnet. SEG 1 protects Network B from Network A. SEG 2 protects Network C from Network A. Each security gateway has two Ethernet network interfaces (Port A and Port B), which are used to pass traffic between networks.

A dynamic security policy "includes any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to that [sic] criteria."[4]

Figure 5 shows some of the 1,888 filters that are available by default on the TippingPoint IPS. These filters can be adjusted to perform various user-defined transformation functions (such as allowing, blocking, logging, and/or copying) on packets corresponding to the relevant criteria.[5]

[4] '205 Patent, Column 4, Lines 43–47.

[5] See, "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 23, Section 3 "Filters."

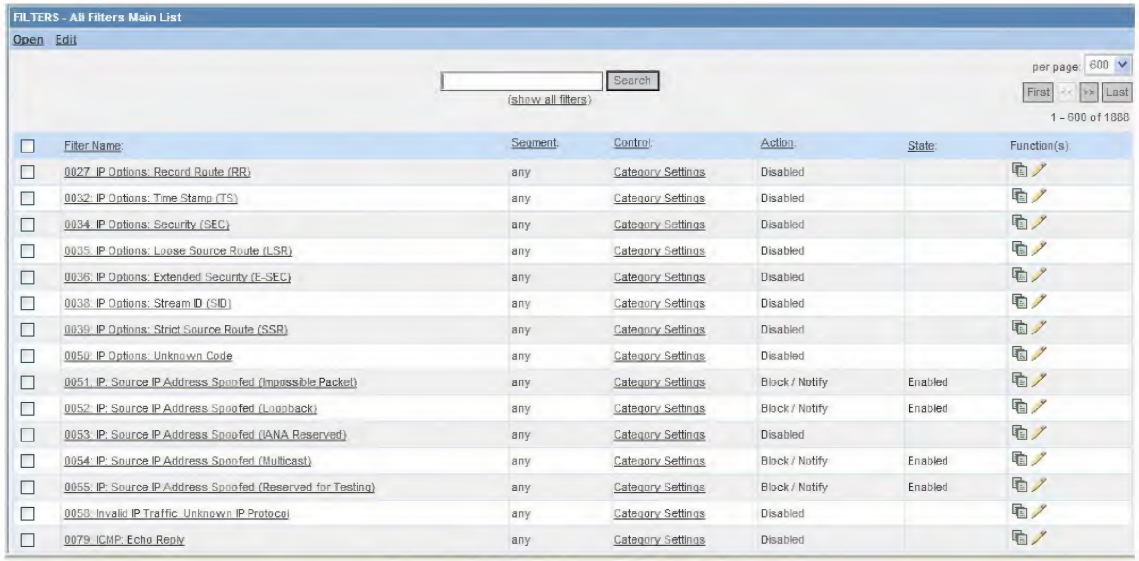


Figure 5: Sample filters available in the IPS.

Each of these independent filters can be set to a series of actions that either block or permit the packet. An example filter is shown in Figure 6—filter 0361: "HTTP Protected File Access (/etc/passwd)." The "save" button in the lower right corner updates the filter settings.

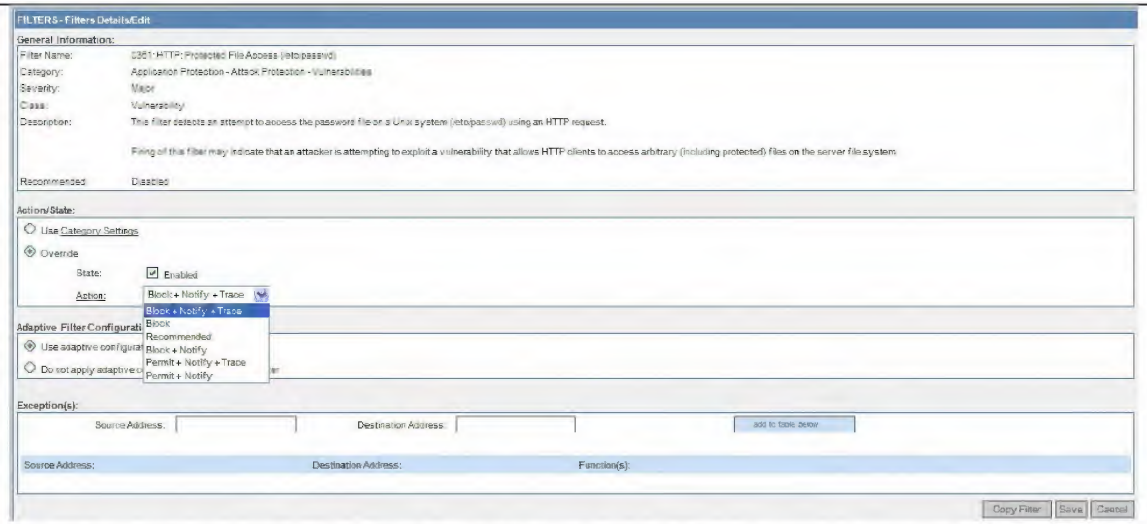
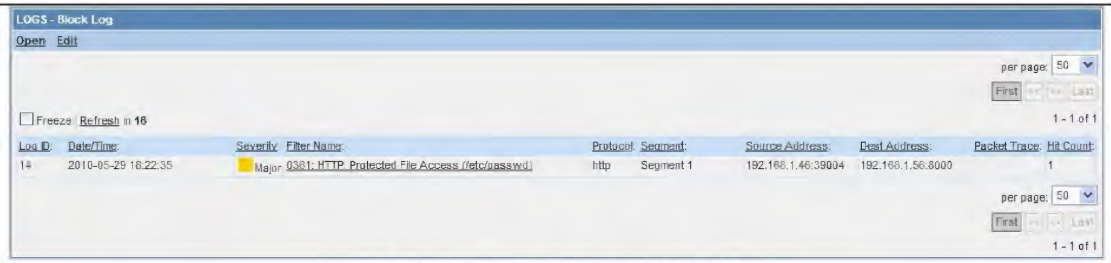


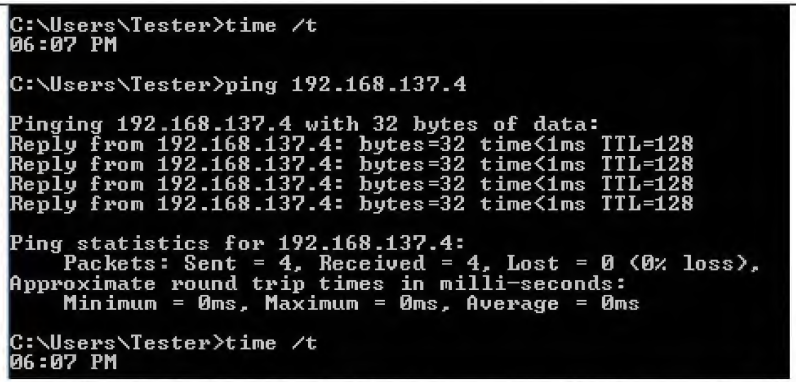
Figure 6: Filter 0361, which "detects an attempt to access the password file on a Unix system (/etc/passwd) using an HTTP request." A series of actions are possible for packets that are identified by this filter.

The HTTP protected file access filter applies to application-layer packet-header information. In this case the application-layer protocol is HTTP and the header information is the method (e.g., GET) and the URL path ("/etc/passwd").

As shown in Figure 6, the action taken by this filter can be set to "Block + Notify + Trace," which applies a packet transformation function to each packet that matches the application-layer packet-header pattern.

Blocked packets are intercepted and logged in a Block Log, as is shown in Figure 7, after a single packet that matches the 0361:HTTP:Protected File Access (/etc/passwd) filter criteria while the appropriate action was set, thus demonstrating that a packet digest logging function is included in the packet transformation function performed on the HTTP application-layer packet-header information.

	 **Figure 7: Block Log, which shows the blocked packets.** Thus, as explained above, The TippingPoint system may contain a "plurality of packet security gateways associated with a security policy management server," wherein the packet security gateways receive "a dynamic security policy" from the TippingPoint LSM and associated web server, "that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information." Specifically, 0361:HTTP:Protected File Access (/etc/passwd) filter implements such a rule that can perform a packet digest logging function on packets comprising the application-layer packet-header information.
1b. receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	The TippingPoint system performs a method, comprising: receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway. To demonstrate this, Exponent utilized the test configuration setup shown in Figure 4 and attempted to ping Computer B from Computer A, which are located on opposite sides of the packet security gateway interface SEG 1. These ping requests were allowed to transmit indicating the security gateway interface was forwarding packets from Computer B to Computer A as well as Computer A to Computer B. Figure 8 is a screenshot of Computer B's successful attempt to ping Computer A.

	 **Figure 8: Screenshot of ping from Computer A (192.168.137.4) to Computer B (172.16.3.5) indicating 0% packet loss, demonstrating that the security gateway forwarded the packets.** Furthermore, as demonstrated in detail below, HTTP requests contained in TCP/IP packets can also be received by the packet security gateway and can be forwarded or dropped. Thus, it has been demonstrated that one of the packet security gateways (i.e., SEG 1) on the TippingPoint IPS receives packets associated with a network protected by the packet security gateway. Therefore, the TippingPoint system anticipates the method of claim element 1b.
1c. identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information;	The TippingPoint system performs a method, comprising: identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information. To demonstrate this functionality of the TippingPoint IPS, two computers were set up on a simplified test network, configured as shown in Figure 9.

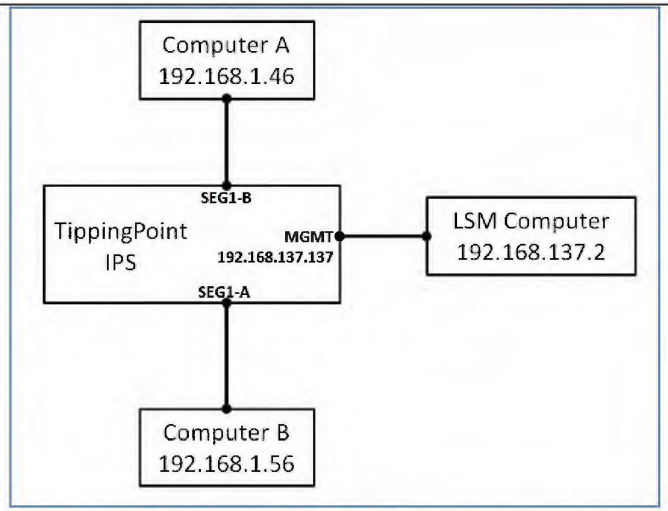


Figure 9: Network map of test network illustrating connectivity of the TippingPoint IPS, Computer A, Computer B, and the LSM Computer.

In this test network, one computer was configured to operate as an HTTP client and one was configured to operate as an HTTP server. Computer B at network IP address 192.168.1.56 was configured to host a HTTP server.[6] Computer A at network IP address 192.168.1.46 was used to make HTTP GET requests to attempt to access the URL path "/etc/passwd" on the HTTP server. That is, Computer A played the role of an HTTP client.

The packets containing the GET Method and the URL "192.168.1.46/etc/passwd" are identified by that application-layer packet-header information.[7]

---

[6] Exponent used a python programming language via a python language interpreter and standard python module called "http.server" to run an HTTP server on Computer B. For additional information, see https://docs.python/org (generally) as well as https://docs.python.org/2/library/simplehttpserver.html and https://docs.python.org/3/library/http.server.html.

[7] See, for example, US 9565213 at 21:56-64: "In some embodiments, identifying the packets comprising the application-layer packet-header information may include the packet security gateway determining that the packets are among the HTTP packets identified by the rule(s) (e.g., the HTTP GET method call

	Initially, the TippingPoint IPS was configured to "Permit + Notify" for the 0361 filter, which corresponds to the "HTTP: Protected File Access" threat. While the TippingPoint IPS was configured to "Permit + Notify" this threat, a first packet, including an HTTP GET request for the URL path "/etc/passwd," was sent by Computer A to the IP address associated with Computer B. During this testing, the HTTP server on Computer B was configured to serve web pages on port 8000 rather than port 80.[8] To send the HTTP GET request, the program "netcat" was used. The netcat program is a well-known utility[9] for sending data using the TCP/IP protocol, which we used to send HTTP requests.[10] We used the netcat utility rather than a more complex web browser (e.g., Chrome or Internet Explorer) to have more fine-grained control over the test packets that were sent. A terminal window display from Computer A is shown in Figure 10. This figure shows (1) the use of netcat (the command line invocation of netcat is performed via the "nc" command) on Computer A to connect to port 8000 on Computer B (first line); (2) the HTTP GET request for the "etc/passwd" path (second line); (3) the HTTP response from the web server at Computer B indicating that the file was not found (remaining lines).

and/or the HTTP PUT method call may specify one or more URIs, and packet security gateway 112 may determine that the packet(s) originated from and/or are destined for a network address corresponding to the URI(s))."

8 Port 8000 is the default port used by the python http server module.

9 See, for example, http://netcat.sourceforge.net/ and https://nmap.org/ncat/.

10 HTTP is an application layer protocol that typically runs on top of the lower-level TCP protocol.

```
exponent@adam-jumpkit:~$ nc 192.168.1.56 8000
GET /etc/passwd HTTP/1.1

HTTP/1.0 404 File not found
Server: SimpleHTTP/0.6 Python/3.4.2
Date: Wed, 30 May 2018 01:20:41 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Content-Length: 452

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 404</p>
        <p>Message: File not found.</p>
        <p>Error code explanation: 404 - Nothing matches the given URI.</p>
    </body>
</html>
```

Figure 10: Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, the HTTP GET request for the "/etc/passwd" path, and the response from Computer B indicating that the "etc/passwd" file was not found by the server (thus it responds with a 404 error).

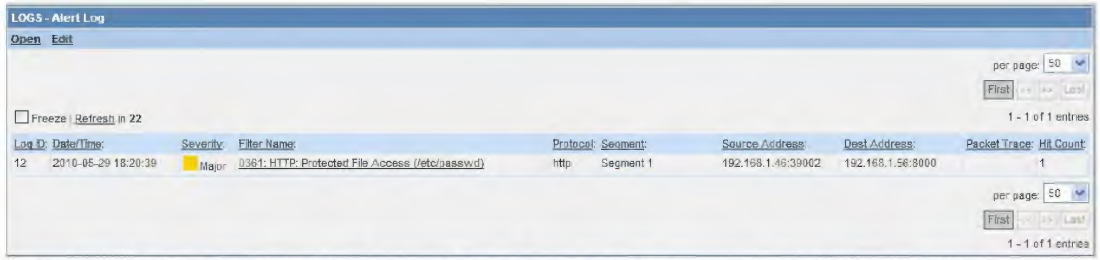
Because the TippingPoint IPS was configured to "Permit + Notify" this threat, the HTTP GET request was allowed to pass from Computer A, through the TippingPoint IPS, and arrive at Computer B. The arrival of the HTTP GET request at Computer B is illustrated in Figure 11, which shows that the GET request for the path "/etc/passwd" invokes an HTTP code 404 response because the file "/etc/passwd" is not available on the HTTP server. The 404 response also appears back at the HTTP client on Computer A, as demonstrated in Figure 10.

```
C:\Users\Tester\Desktop\web>python -m http.server
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.46 - - [29/May/2018 18:20:41] code 404, message File not found
192.168.1.46 - - [29/May/2018 18:20:41] "GET /etc/passwd HTTP/1.1" 404 -
```

Figure 11: Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server has sent back an HTTP code 404 in response to the GET request for "/etc/passwd."

CENTRIPETAL-CSCO 088006

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 506

	As Figure 12 illustrates, the "Alert Log" on the LSM GUI records that the first packet was detected and allowed to continue to the destination.[11] Specifically, Figure 12 shows that the HTTP attack packet associated with the 0361 filter was received from the source 192.168.1.46 (Computer A) and allowed to continue to destination 192.168.1.56 (Computer B).  LOGS - Alert Log Open Edit per page: 50 First Freeze | Refresh in 22 1 - 1 of 1 entries Log ID: Date/Time: Severity: Filter Name: Protocol: Segment: Source Address: Dest Address: Packet Trace: Hit Count: 12 2010-05-29 18:20:39 Major 0361: HTTP: Protected File Access (/etc/passwd) http Segment 1 192.168.1.46:39002 192.168.1.56:8000 1 per page: 50 First 1 - 1 of 1 entries **Figure 12: Screenshot from the TippingPoint LSM GUI showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was allowed.** Thus, it has been demonstrated that the packet security gateway SEG 1 of the Tipping Point IPS identifies "one or more packets comprising the application-layer packet-header information," on a packet-by-packet basis, "from amongst the packets associated with the network protected by the packet security gateway," thereby satisfying the requirements of the method described in claim element 1c.
1d. performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet	The TippingPoint system performs a method, comprising: performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises. As shown in the analysis of claim element 1c above, the TippingPoint system can log attack packets based on identifying application-layer packet-header information. The TippingPoint system can perform other packet transformation functions as well. For example, the packets can also be blocked. For example, as shown in Figure 13, the TippingPoint IPS was configured to "Block + Notify" the same HTTP threat corresponding to the 0361 filter. Then a second packet, including an HTTP GET request for

[11] See "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005) section "Alert Log" starting on p. 115.

CENTRIPETAL-CSCO 088007

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 507

transformation function comprises	the URL path "/etc/passwd," was sent by Computer A to the IP address associated with Computer B.

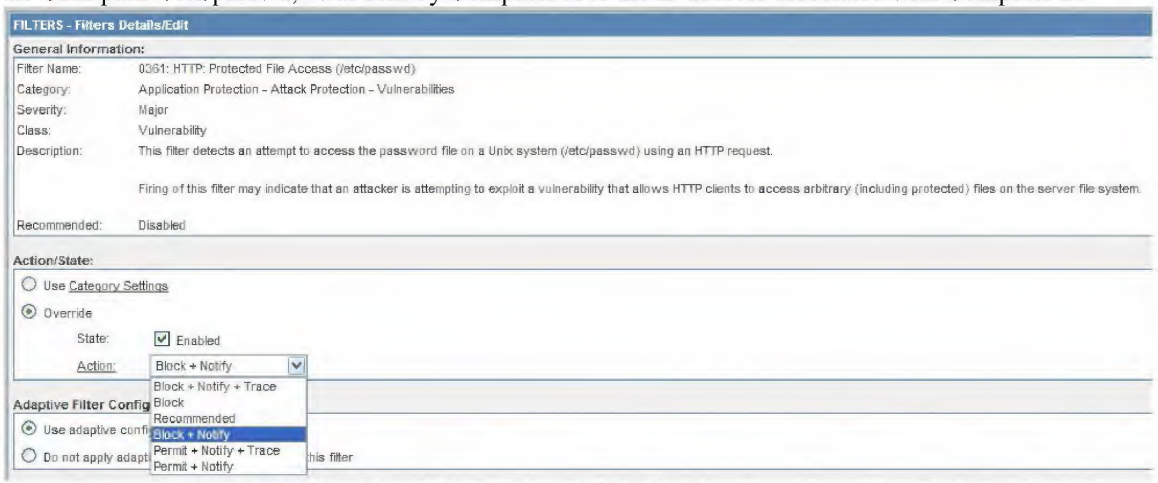


Figure 13: Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from "Permit + Notify" to "Block + Notify."

Figure 14 shows a terminal window display from Computer A. Specifically, it shows (1) the use of netcat (the command line invocation of netcat is performed via the "nc" command) on Computer A to connect to port 8000 on Computer B (first line); (2) the HTTP GET request for the "etc/passwd" path (second line); and (3) the absence of any HTTP response from the web server at Computer B and subsequent shutdown of the HTTP client using the "Ctrl-C" keyboard combination to send the client process a kill signal.

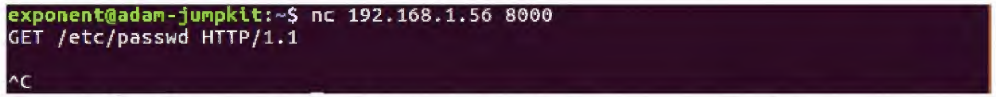


Figure 14: Screenshot from Computer A showing the terminal window for the netcat session. This figure shows the initial connection from Computer A to Computer B, and the HTTP GET request for the "/etc/passwd" path. It also illustrates that no response was received from Computer B (because Computer B never received the request).

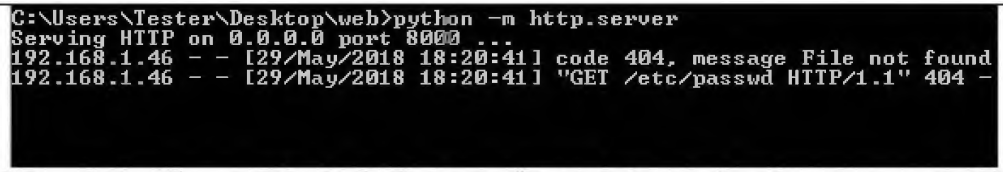
Figure 15 illustrates the "Block Log" on the LSM GUI, which shows that the second packet was detected and blocked by the TippingPoint IPS packet filter.[12] More specifically, Figure 15 shows that the HTTP attack packet associated with the 0361 filter was received from source 192.168.1.46 (Computer A) and blocked from continuing to destination 192.168.1.56 (Computer B).

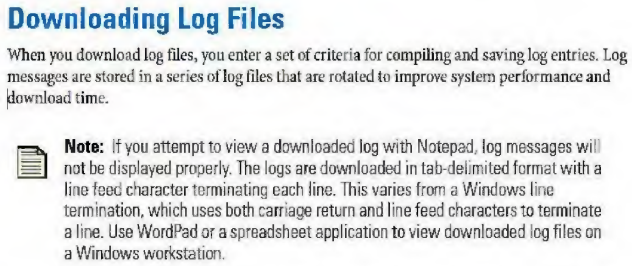


Figure 15: Screenshot from the TippingPoint LSM GUI, showing that the packet corresponding to the HTTP protected file access attack and the 0361 packet filter was blocked.

Because the TippingPoint IPS was configured to "Block + Notify" this HTTP file access threat prior to the arrival of the second packet, the HTTP GET request was *not* allowed to pass from Computer A through the TippingPoint IPS. Therefore, this packet never arrived at Computer B. The lack of arrival (i.e., being blocked) is illustrated in Figure 16, which shows the same text as Figure 11. The figure also shows additional whitespace, indicating that the request was not received; had the request been received, there would be a second code 404 response logged to the terminal windows as well as a second GET request logged to the terminal window; however, no such log lines were displayed.

[12] See "UnityOne Local Security Manager User's Guide," version 2.1 (copyright 2005) section "Block Log" starting on p. 116.

	 **Figure 16: Screenshot from Computer B showing the Windows "cmd" terminal window for the python web server session. The HTTP server is running on port 8000; the web server did not send back any additional response because it did not receive the second packet. (The response shown in the figure is the response to the first packet.)** Therefore, it has been demonstrated that the packet security gateway of the TippingPoint IPS performs a packet transformation function on the packets comprising the application-layer packet-header information, thus satisfying the requirements of the method described in claim element 1d.
1e. identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;	The TippingPoint system performs a method, comprising performing the packet transformation function, wherein the performing comprises: identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information. As shown in the analysis of claim elements 1a, 1c, and 1d above, the packet transformation function includes not only blocking and/or forwarding, but also packet digest logging functionality. See, for example, Figure 15, which shows the "Block Log" for the blocked packet. The Block Log contains subset of the packet information, e.g., sounds IP/port and destination IP/port are shown in Figure 15, which is a subset of the packet information of the blocked application-layer packet. Therefore the TippingPoint system satistifes all requirements of claim element 1e.
1f. generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet	The TippingPoint system performs a method, comprising performing the packet transformation function, wherein the performing comprises: generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function. As shown in the analysis of claim elements 1a, 1c, and 1d above, the packet transformation function includes not only blocking and/or forwarding, but also record generation functionality. See, for example, Figure 15, which shows the "Block Log" for the blocked packet. The row of data shown in the Block Log

digest logging function; and	for the blocked packet is a record that was generated for logging the blocked attack event. Therefore the TippingPoint system satistifes all requirements of claim element 1f.
1g. reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and	The TippingPoint system performs a method, comprising performing the packet transformation function, wherein the performing comprises: reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard. As shown in the analysis above, the TippingPoint IPS logs attack packets. For example, the "Block Log" shown in Figure 15 will contain a row of data for each blocked attack packet. The TippingPoint IPS logs can be managed using the LSM GUI.[13] Log entries can be downloaded and saved.[14] According to the TippingPoint documentation, downloaded log entries can be reformatted as tab-delimited lines of data terminated with a line-feed character, as shown in Figure 17, which shows a screen capture from the LSM User's Guide.[15]  **Downloading Log Files** When you download log files, you enter a set of criteria for compiling and saving log entries. Log messages are stored in a series of log files that are rotated to improve system performance and download time. **Note:** If you attempt to view a downloaded log with Notepad, log messages will not be displayed properly. The logs are downloaded in tab-delimited format with a line feed character terminating each line. This varies from a Windows line termination, which uses both carriage return and line feed characters to terminate a line. Use WordPad or a spreadsheet application to view downloaded log files on a Windows workstation. **Figure 17: Screen Capture from LSM User Manual indicating that logs can be downloaded in tab-separated format.** In addition, the IPS logs can be downloaded as .csv files from the TippingPoint test system. The .csv files are reformatted versions of the log files.

[13] See, "TippingPoint UnityOne Local Security Manager User's Guide" version 2.1 (copyright 2005) at p. 113, section "Log."
[14] Ibid, at page 122.
[15] Ibid

CENTRIPETAL-CSCO 088011

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 511

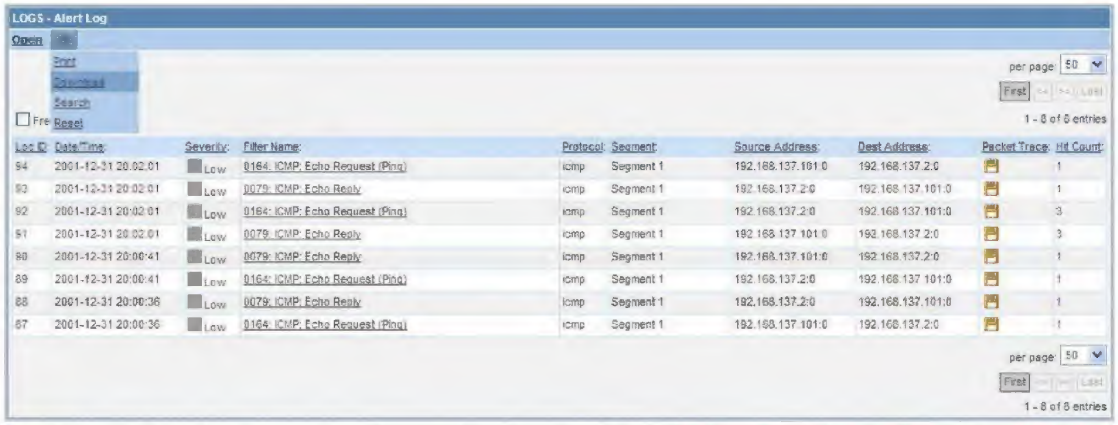


Figure 18: A log of packets sent from Computer B to Computer A, including the option to download (in the Edit menu).

The LSM GUI includes an option to choose a .csv file or not during download.

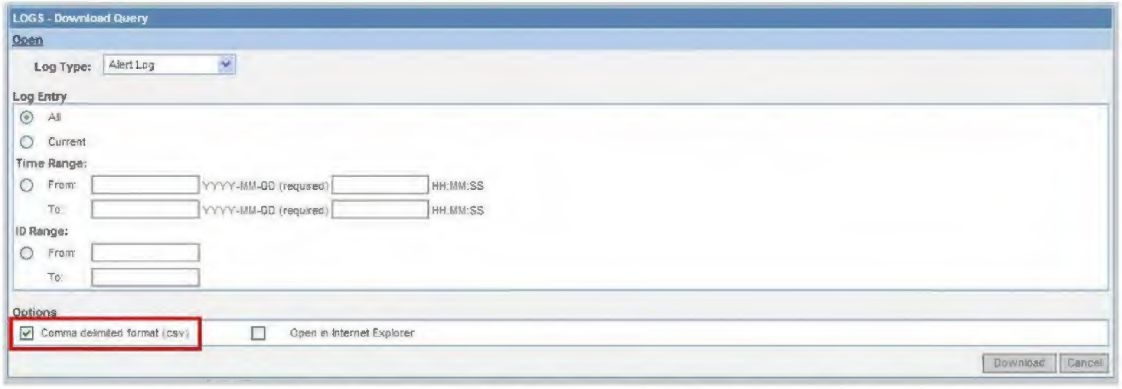


Figure 19: Download options, including specific time ranges and an option to download a .csv formatted log.

And finally, the downloaded .csv files can be opened in Microsoft Excel to view their contents.

CENTRIPETAL-CSCO 088012

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 512

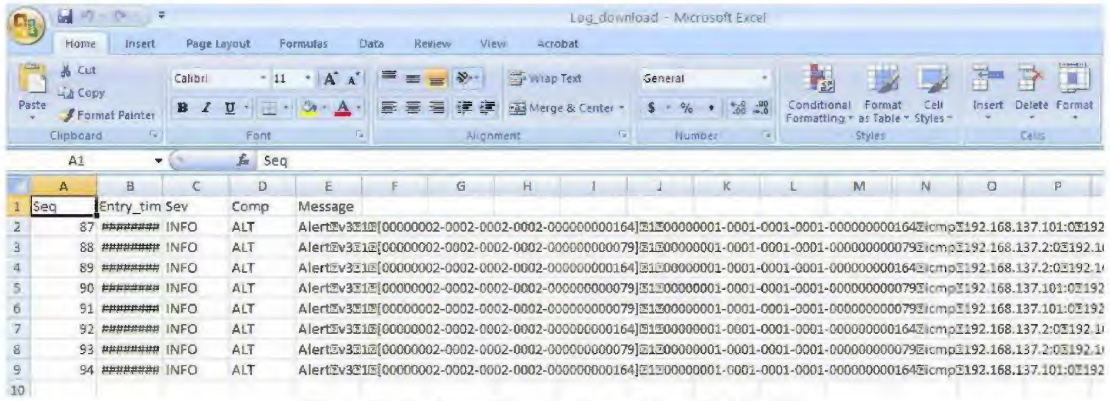
	 Log_download - Microsoft Excel Seq Figure 20: Contents of downloaded .csv formatted log file. Therefore the TippingPoint system satisfies all requirements of claim element 1g.
1h. routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.	The TippingPoint system performs a method, comprising: routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function. As shown in the analysis of claim element 1a above, the TippingPoint IPS can be configured to "Block+Notify+Trace" the packet corresponding to the HTTP protected file access network threat. The "Trace" functionality records a copy of the attack packet to a log server, i.e., the packet is routed to a monitoring device. For example, when this functionality is enabled the "Block Log" will show an entry in the "Packet Trace" column, as seen in Figure 21.



Figure 21: Screenshot from the LSM GUI showing the Block Log, which lists packets that were not forwarded to their intended destination.

By downloading the packet trace (see "Packet Trace" column in Figure 21) and opening it in Wireshark,[16] Exponent was able to view the contents of the packet (see Figure 22).

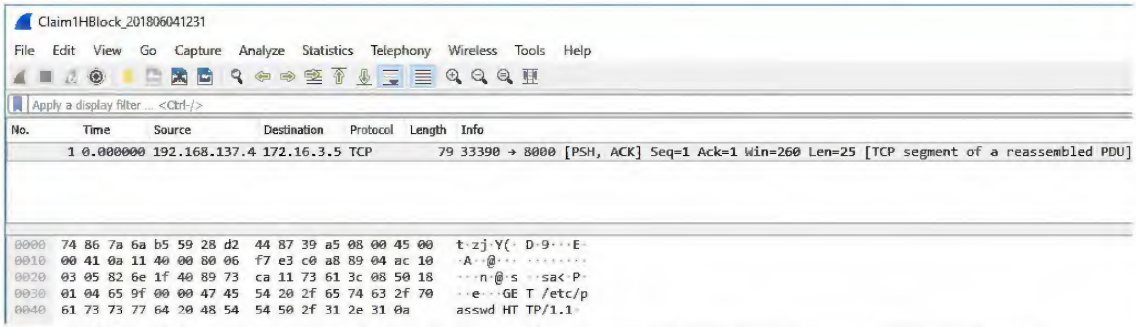


Figure 22: Packet information logged by the TippingPoint system. For example, the ASCII characters "GET /etc/passwd HTTP/1.1" can be seen in the lower right section of this figure.

The application-layer packet information can be seen in Figure 22. For example, the string "GET /etc/passwd" is seen in the lower right of the figure.

Thus, the TippingPoint IPS packet security gateway can filter network traffic on a packet-by-packet basis, and perform a packet transformation on packets corresponding to the application-layer packet-header

[16] Wireshark is a network analysis computer program. See, for example, https://www.wireshark.org.

CENTRIPETAL-CSCO 088014

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 514

	information, wherein said packets are routed to a monitoring device. As such, the TippingPoint IPS satisfies the requirements of claim element 1h.

Claim 3 analysis

Claim 3	Analysis of TippingPoint IPS
3. The method of claim 1, wherein the at least one rule indicates performing a deny packet transformation function on the packets comprising the application-layer packet-header information, and wherein the performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information.	The TippingPoint system performs the method of Claim 1, wherein the at least one rule indicates performing a deny packet transformation function on the packets comprising the application-layer packet-header information, and wherein the performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information. See analysis of claim elements 1a and 1d. In the analysis of this element. The TippingPoint filter corresponding to the application-layer packet-header information is configured to "Block+Notify+Trace," in claim element 1a, and "Block+Notify," in claim element 1d. These configurations both block the attack packet, which constitutes a "deny packet transformation function." In both cases, the packet is dropped by the packet security gateway (i.e. SEG 1) rather than being allowed to continue to its destination. Therefore the TippingPoint system satisfies all requirements of Claim 3.

APPENDIX G

'856 Patent Analysis

Check Point R77

Contents

Claim 1 Analysis 3
Claim 18 Analysis 24
Claim 24 Analysis 25
Claim 25 Analysis 27

Claim 1 Analysis

Claim 1	Analysis of Check Point R77
1a. A method comprising: receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;	Check Point R77 is a commercial software product comprising a security management server (SMS) program,[1] which when installed on suitable hardware constitutes a security policy management server, and a security gateway (SG) program,[2] which when installed on suitable hardware constitutes of a packet security gateway. Check Point R77 also utilizes a graphical user interface (GUI) for the SMS. The security gateway and SMS include a processor and memory and are configured to filter packets in accordance with a plurality of packet filtering rules. To demonstrate the functionality of the system, Exponent set up a test network (see Figure 1 and Figure 2) to send traffic across the security gateway (labeled as "gw2" in the figures). the components labeled "SMS", "GUI", and "gw2" in Figure 2 collectively form "the Check Point R77 system." The Check Point R77 system performs a method comprising: receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat.

[1] See "Check Point R77 Security Management Server Administration Guide" (dated Aug 27, 2013).
[2] See "Check Point R77 Firewall Administration Guide" (dated Aug 27, 2013).

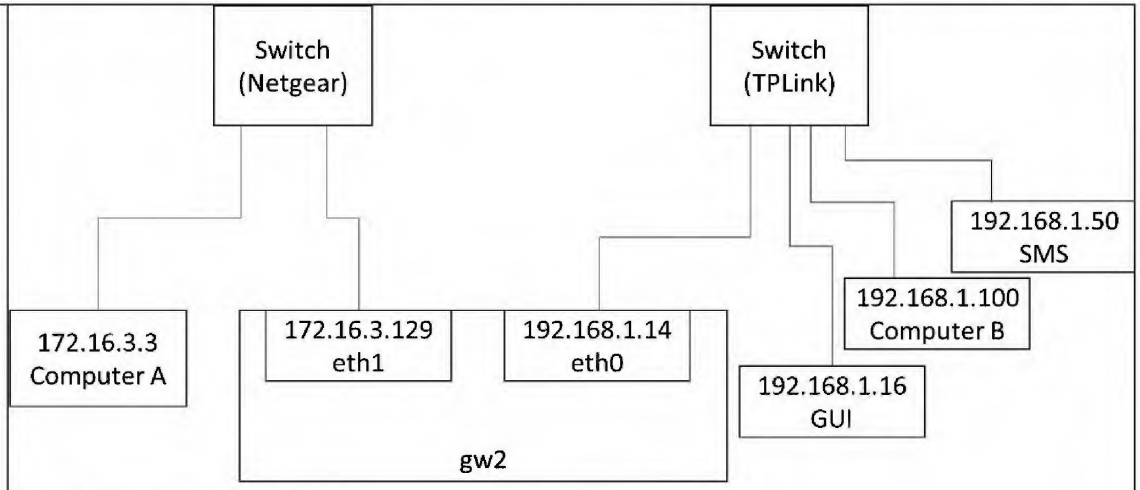


Figure 1: Network diagram of test setup

Exponent installed the Check Point R77SMS product on a 32-bit PC-compatible Dell Latitude E6400 computer using the "Check_Point_R77.20_T124_Install.Gaia.iso" DVD ISO image (see "SMS" in Figure 2).[3]

Exponent also installed the Check Point R77 SG product on a 32-bit PC-compatible Dell PowerEdge 1750 computer using the "Check_Point_R77.20_T124_Install.Gaia.iso" DVD ISO image (see "gw2" in Figure 2). Thus, the Check Point R77 packet filtering system comprises "a hardware processor and a memory."

[3] According to the Check Point website, DVD installation material was available in December 2010 (see https://supportcenter.CheckPoint.com/supportcenter/) and the installation procedure for the Firewall and Security Management Server is documented in the "R75 Installation and Upgrade Guide."

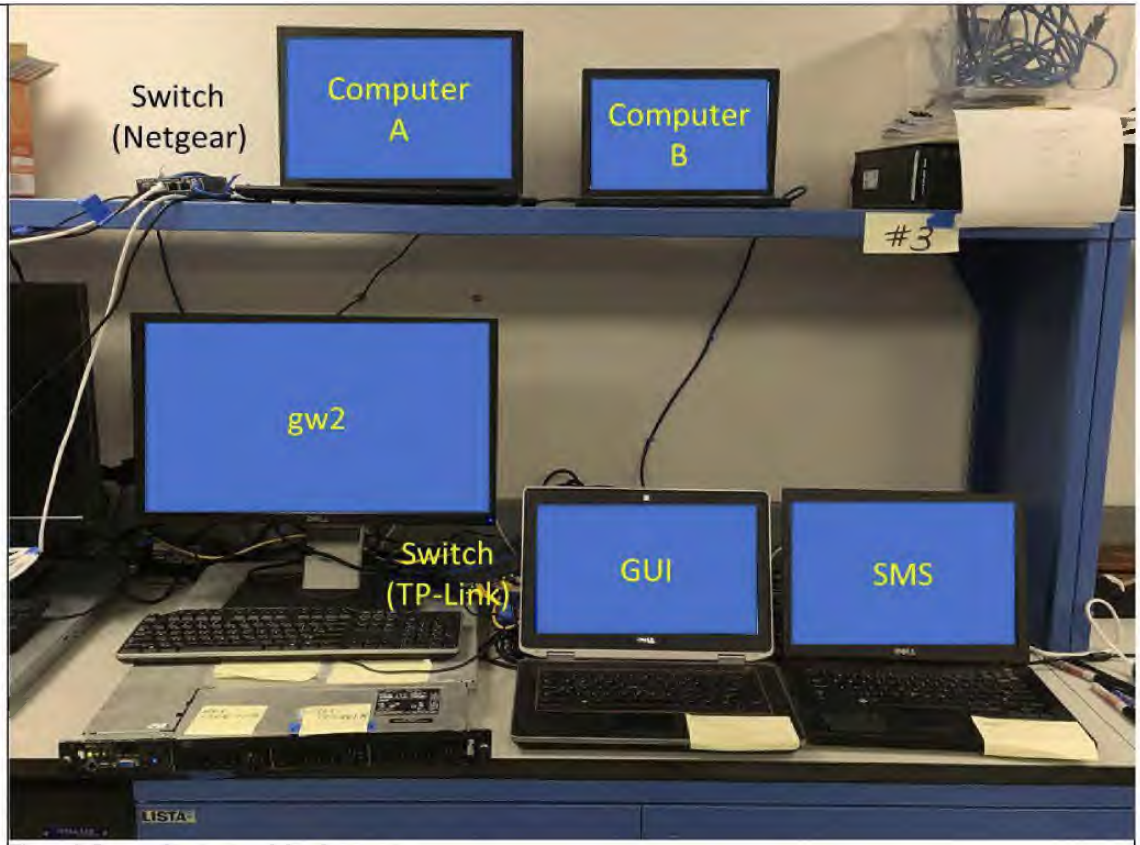


Figure 2: Image of test network hardware setup.

The Check Point R77 system provides the ability to install a plurality of packet filtering rules, including blocking for specific domain names. Exponent defined a domain-specific blocking rule for a domain named "patent856.com", as shown in Figure 3. Thus, one of the network-threat indicators received by the Check Point R77 packet-filtering system comprises a domain name identified as a network threat.

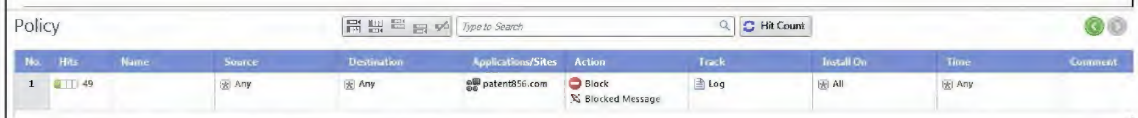


Figure 3: Rule blocking the "patent856.com" domain.

Numerous other rules pertaining to numerous other network threat indicators are also installed by default on the Check Point R77 system, as shown in Figure 4. Figure 4 demonstrates that the Check Point R77 system is not limited to receiving a single packet filtering rule, but can in fact receive a plurality of such rules corresponding to various network threats.

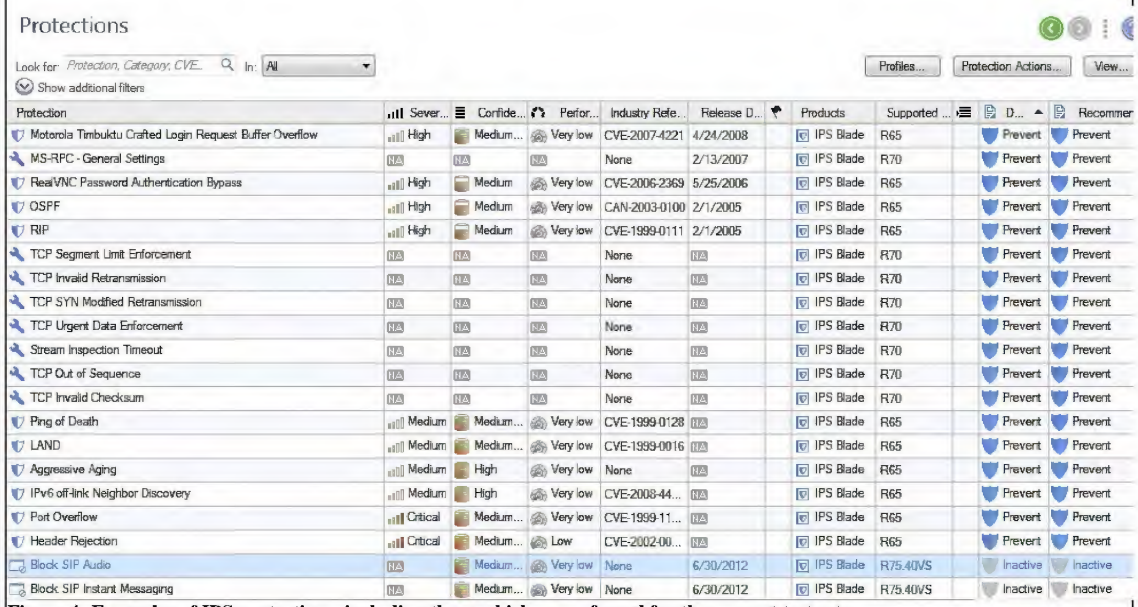


Figure 4: Examples of IPS protections, including those which are enforced for the current test setup.

Exponent also set a final rule for the firewall to accept packets that are not blocked by any of the other

rules of the system (Figure 5).



Figure 5: Screenshot showing a final allow rule, which applies to any traffic that is not blocked by the other rules.

Domain-specific blocking using HTTP:

Computer A (IP 172.16.3.3) was used to host an HTTP server, using the python SimpleHTTPServer module.

The "hosts" file on Computer B was then used to route traffic for a given domain to a specific IP address. In the example in Figure 6, the "Patent856.com" domain name is associated with the IP address of Computer A.

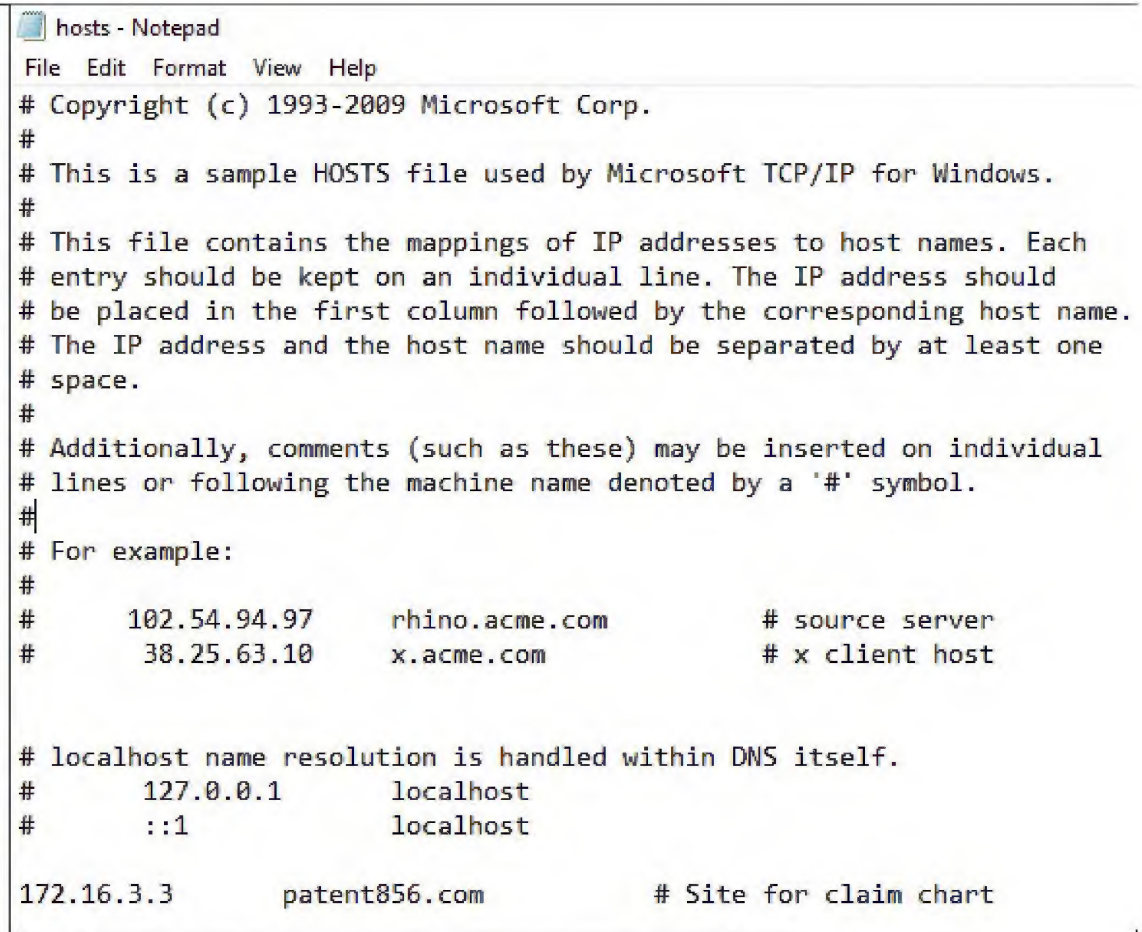


Figure 6: Hosts file relating the domain name "patent856.com" to the IP address 172.16.3.3

The server was hosted on port 8000 of Computer A, as shown in Figure 7 below:

```
exponent@adam-jumpkit:~/Desktop/https_server$ python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
```

Figure 7: Hosting on Port 8000 of Computer A

The hosts file in Computer B was then modified to direct traffic from "patent857.com" to IP address 172.16.3.3, as shown in Figure 8. When "http://patent857.com:8000" was typed into a web browser on Computer B, the webpage hosted on Computer A was accessed successfully (Figure 9).

```
172.16.3.3        patent857.com              # Site for claim chart
```

Figure 8: Initial test set up for the hosts file to associate the domain name "patent857.com" with IP address 172.16.3.3

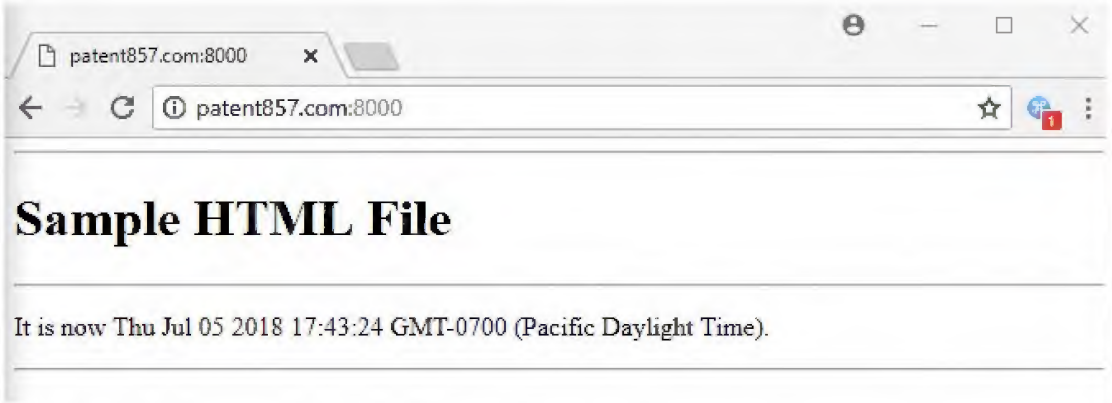


Figure 9: Display from Computer B of the HTML file hosted on Computer A

Next, the hosts file was modified to route requests for "patent856.com" to IP address 172.16.3.3 (Figure 10).

	172.16.3.3 patent856.com # Site for claim chart **Figure 10: Modification to the hosts file to associate the domain name "patent856.com" with the IP address 172.16.3.3.** In this case, because the domain name is "patent856.com" rather than "patent857.com" access to the HTML page is blocked by the gateway (Figure 11). As shown in Figure 11, because the access was blocked, the request is re-routed and a default page from a different machine is displayed rather than the HTML page hosted on Computer A.

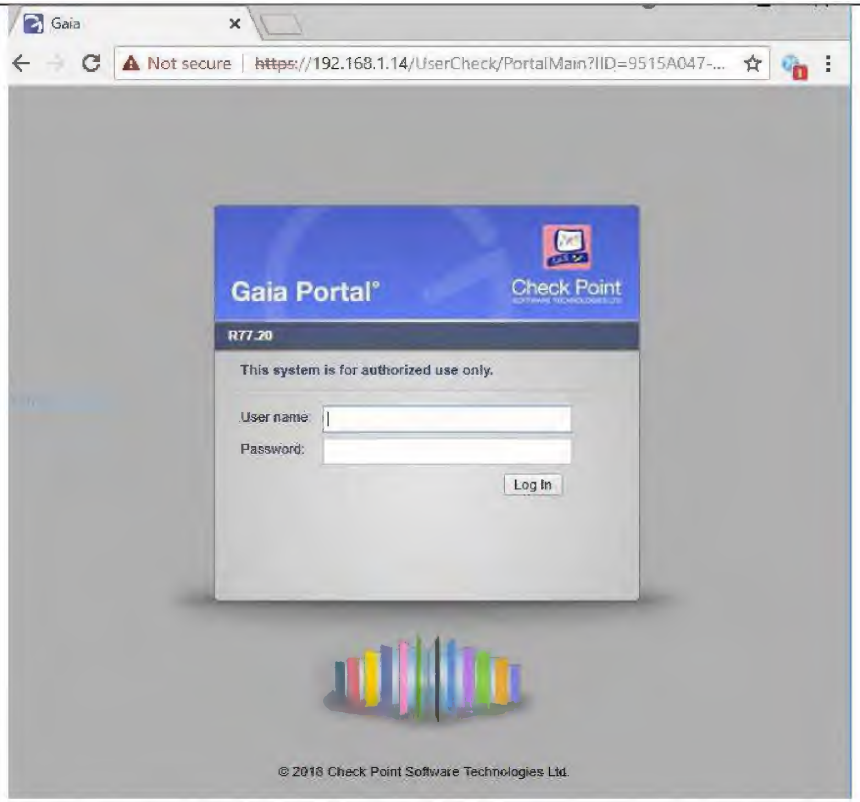


Figure 11: Screenshot from Computer A indicating that access to the "patent856.com" domain was blocked by the gateway.

Thus, Exponent's testing has shown that the Check Point R77 system performs a method where the packet filtering system (which comprises "a hardware processor and a memory") is configured to filter packets in accordance with multiple packet-filtering rules. The packet-filtering system receives "data indicating a plurality of network-threat indicators," and one of these indicators comprises "a domain name identified as a network threat."

1b. identifying packets comprising unencrypted data;	The Check Point R77 system performs identifying packets comprising unencrypted data. The Check Point R77 system operates a method that satisfies the requirements of claim element 1a, as described above, and furthermore includes identifying packets comprising unencrypted data. This is most effectively illustrated by demonstrating the manner in which the transmission of both encrypted and unencrypted data packets can be selectively blocked or allowed by a packet filtering device in the Check Point R77 system. Using the test setup described above, Exponent demonstrated that the Check Point R77 system enables the ability to block encrypted HTTPS traffic, which can be accomplished by de-selecting "Categorize HTTPS sites" in the firewall options menu of the SMS GUI (Figure 12).  **Figure 12: HTTPS sites are not categorized.** Using the python modules "SimpleHTTPServer," "BaseHTTPServer," and "ssl," Exponent hosted an HTTPS site on Computer A (Figure 13), which was successfully accessed by Computer B at the patent856.com domain (Figure 14).  **Figure 13: HTTPS server hosted on Computer A**

CENTRIPETAL-CSCO 088028

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 528

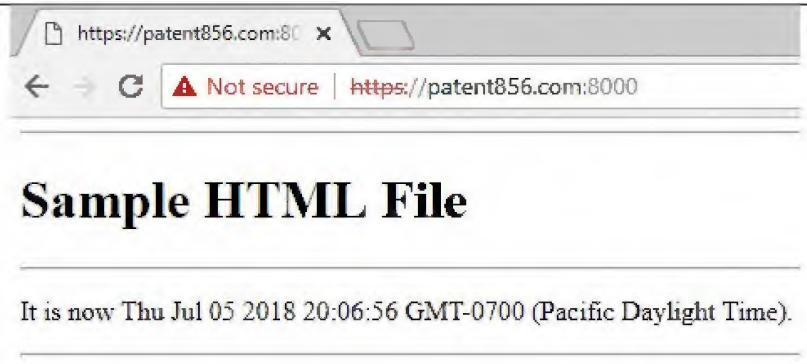


Figure 14: Successful loading of HTTPS site

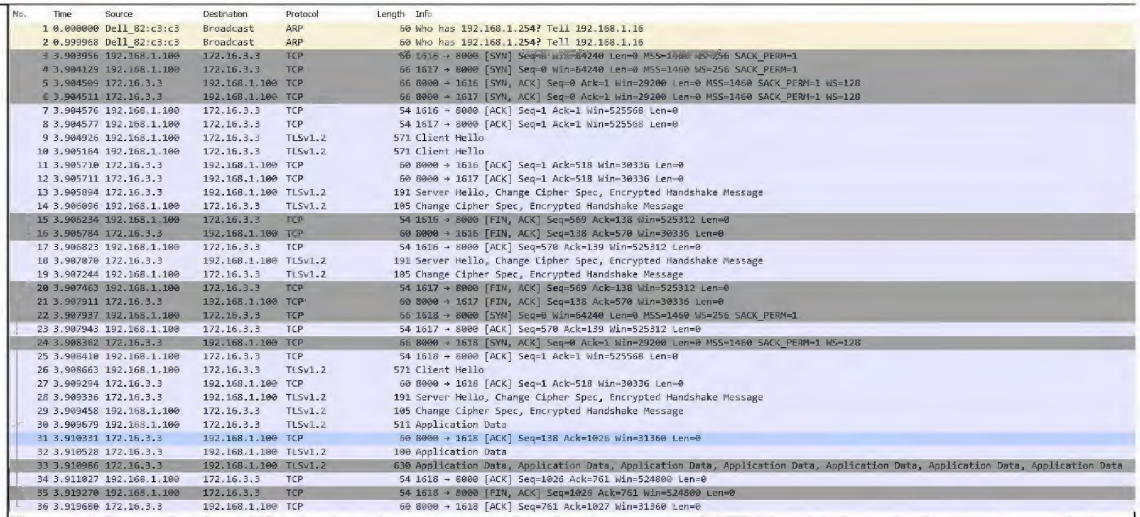
The Python server on Computer A shows a successful access by Computer B (Figure 15):

```
exponent@adam-jumpkit:~/Desktop/https_server$ python -m https_server
Enter PEM pass phrase:
192.168.1.100 - - [05/Jul/2018 20:05:16] "GET / HTTP/1.1" 200 -
```

Figure 15: Computer B successfully accessed HTTPS site hosted son Computer A.

Wireshark[4] (Figure 16) was then used to show the successful communication of unencrypted packets (during and prior to completion of the TLS handshake) as well as the encrypted packets (transmitted after completion of the TLS handshake).

[4] Wireshark is a network analysis computer program. See, for example, https://www.wireshark.org.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_82:c3:c3	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.16
2	0.999968	Dell_82:c3:c3	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.16
3	3.903956	192.168.1.100	172.16.3.3	TCP	58	1615 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	3.904129	192.168.1.100	172.16.3.3	TCP	66	1617 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	3.904509	172.16.3.3	192.168.1.100	TCP	66	8000 → 1616 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
6	3.904511	172.16.3.3	192.168.1.100	TCP	66	8000 → 1617 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
7	3.904576	192.168.1.100	172.16.3.3	TCP	54	1616 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0
8	3.904577	192.168.1.100	172.16.3.3	TCP	54	1617 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0
9	3.904926	192.168.1.100	172.16.3.3	TLSv1.2	571	Client Hello
10	3.905164	192.168.1.100	172.16.3.3	TLSv1.2	571	Client Hello
11	3.905710	172.16.3.3	192.168.1.100	TCP	60	8000 → 1616 [ACK] Seq=1 Ack=518 Win=30336 Len=0
12	3.905711	172.16.3.3	192.168.1.100	TCP	60	8000 → 1617 [ACK] Seq=1 Ack=518 Win=30336 Len=0
13	3.905894	172.16.3.3	192.168.1.100	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
14	3.906036	192.168.1.100	172.16.3.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
15	3.906234	192.168.1.100	172.16.3.3	TCP	54	1615 → 8000 [FIN, ACK] Seq=569 Ack=138 Win=525312 Len=0
16	3.906784	172.16.3.3	192.168.1.100	TCP	60	8000 → 1616 [FIN, ACK] Seq=138 Ack=570 Win=30336 Len=0
17	3.906823	192.168.1.100	172.16.3.3	TCP	54	1616 → 8000 [ACK] Seq=570 Ack=139 Win=525312 Len=0
18	3.907070	172.16.3.3	192.168.1.100	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
19	3.907244	192.168.1.100	172.16.3.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
20	3.907463	192.168.1.100	172.16.3.3	TCP	54	1617 → 8000 [FIN, ACK] Seq=569 Ack=138 Win=525312 Len=0
21	3.907911	172.16.3.3	192.168.1.100	TCP	60	8000 → 1617 [FIN, ACK] Seq=138 Ack=570 Win=30336 Len=0
22	3.907937	192.168.1.100	172.16.3.3	TCP	66	1618 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	3.907943	192.168.1.100	172.16.3.3	TCP	54	1617 → 8000 [ACK] Seq=570 Ack=139 Win=525312 Len=0
24	3.908362	172.16.3.3	192.168.1.100	TCP	66	8000 → 1618 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
25	3.908410	192.168.1.100	172.16.3.3	TCP	54	1618 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0
26	3.908663	192.168.1.100	172.16.3.3	TLSv1.2	571	Client Hello
27	3.909294	172.16.3.3	192.168.1.100	TCP	60	8000 → 1618 [ACK] Seq=1 Ack=518 Win=30336 Len=0
28	3.909336	172.16.3.3	192.168.1.100	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
29	3.909458	192.168.1.100	172.16.3.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
30	3.909679	192.168.1.100	172.16.3.3	TLSv1.2	511	Application Data
31	3.910331	172.16.3.3	192.168.1.100	TCP	60	8000 → 1618 [ACK] Seq=138 Ack=1026 Win=31360 Len=0
32	3.910528	172.16.3.3	192.168.1.100	TLSv1.2	100	Application Data
33	3.910986	172.16.3.3	192.168.1.100	TLSv1.2	630	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
34	3.911027	192.168.1.100	172.16.3.3	TCP	54	1618 → 8000 [ACK] Seq=1026 Ack=761 Win=524800 Len=0
35	3.913270	192.168.1.100	172.16.3.3	TCP	54	1618 → 8000 [FIN, ACK] Seq=1026 Ack=761 Win=524800 Len=0
36	3.919680	172.16.3.3	192.168.1.100	TCP	60	8000 → 1618 [ACK] Seq=761 Ack=1027 Win=31360 Len=0

Figure 16: Screenshot from Wireshark packet capture session showing a successful TLS handshake and subsequent transmission of encrypted application data.

After showing the successful transmission of HTTPS packets, the "Categorize HTTPS sites" box was selected in the firewall options menu of the SMS GUI (Figure 17).

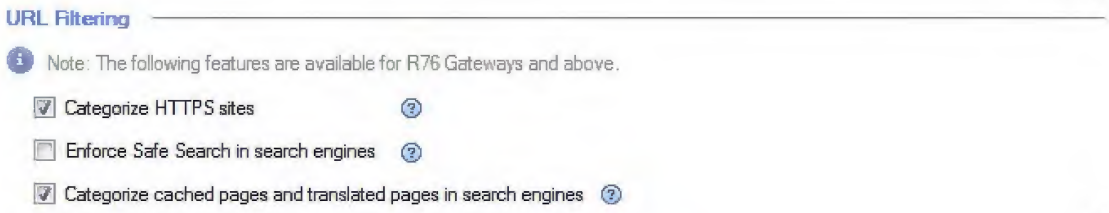
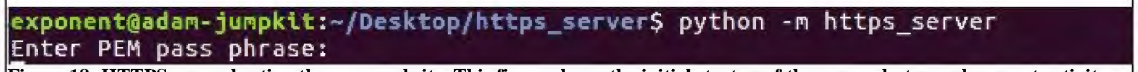


Figure 17: "Categorize HTTPS sites" blocks sites with the HTTPS domain name.

When an attempt was made to access the HTTPS server on Computer A using a browser on Computer

CENTRIPETAL-CSCO 088030

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 530

	B, the page was unable to load (See Figure 18 and Figure 19):  **Figure 18: HTTPS server hosting the same website. This figure shows the initial startup of the server, but no subsequent activity, which indicates that it did not receive any requests from Computer B.**

CENTRIPETAL-CSCO 088031

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 531

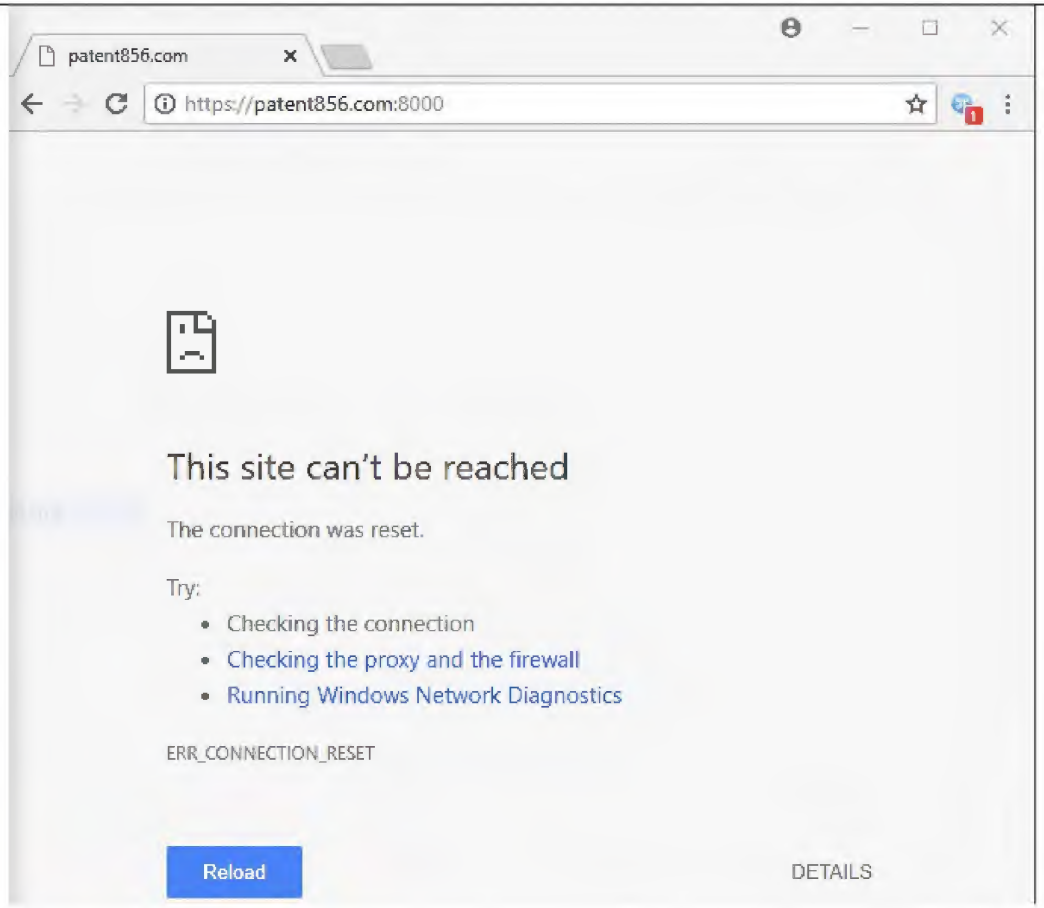
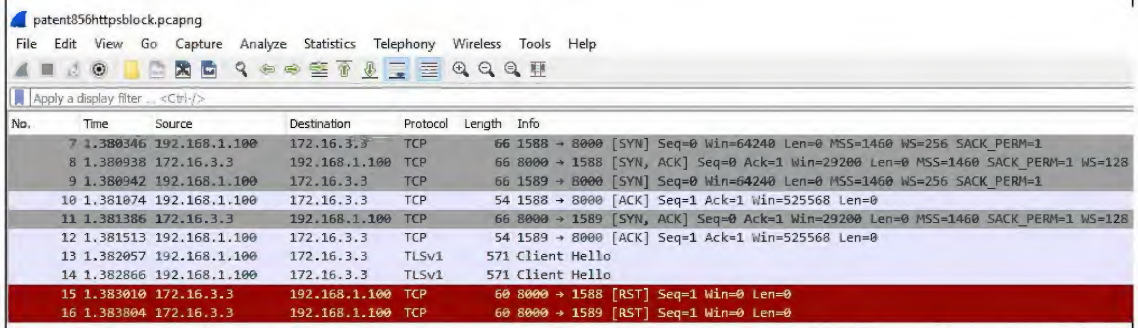


Figure 19: Screenshot of web browser on Computer B indicating blocked access to https://patent856.com:8000

Furthermore, the Wireshark information captured during the blocked attempt to access the HTTPS site shows that the TCP/IP handshake was completed, but the TLS handshake was not completed because

	packets were blocked. For example, the "Client Hello" is still transmitted, but the server does not respond with a "Server Hello" because the packets were blocked.  patent856httpsblock.pcapng File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Apply a display filter ... <Ctrl-/> No. Time Source Destination Protocol Length Info 7 1.380346 192.168.1.100 172.16.3.3 TCP 66 1588 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 8 1.380938 172.16.3.3 192.168.1.100 TCP 66 8000 → 1588 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 9 1.380942 192.168.1.100 172.16.3.3 TCP 66 1589 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 10 1.381074 192.168.1.100 172.16.3.3 TCP 54 1588 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0 11 1.381386 172.16.3.3 192.168.1.100 TCP 66 8000 → 1589 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 12 1.381513 192.168.1.100 172.16.3.3 TCP 54 1589 → 8000 [ACK] Seq=1 Ack=1 Win=525568 Len=0 13 1.382057 192.168.1.100 172.16.3.3 TLSv1 571 Client Hello 14 1.382866 192.168.1.100 172.16.3.3 TLSv1 571 Client Hello 15 1.383010 172.16.3.3 192.168.1.100 TCP 60 8000 → 1588 [RST] Seq=1 Win=0 Len=0 16 1.383804 172.16.3.3 192.168.1.100 TCP 60 8000 → 1589 [RST] Seq=1 Win=0 Len=0 **Figure 20: Screen Capture from Wireshark session running on Computer B showing that the HTTPS server does not respond with a "Server Hello."** Therefore, packets containing unencrypted data, such as the IP addresses in the packet headers, are identified and either blocked or allowed by the Check Point R77 system, as required by claim element 1b.
1c. identifying packets comprising encrypted data;	The Check Point R77 system performs identifying packets comprising encrypted data. The analysis of claim element 1a shows packets containing encrypted data such as the encrypted HTTP application data following the TLS handshake. These packets are identified and blocked or allowed by the Check Point R77 system. In addition, according to the R77 documentation, Encrypted packets can be identified and screened via "HTTPS Inspection" available on Check Point R77. For example, see the following quote (quote shown as indented text below) from page 40 of the "R77 Application Control and URL Filtering Administration Guide": **Predefined Rule** When you enable HTTPS inspection, a predefined rule is added to the HTTPS Rule Base. This rule defines that all

CENTRIPETAL-CSCO 088033

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 533

HTTPS and HTTPS proxy traffic from any source to the internet is inspected on all blades enabled in the Blade column. By default, there are no logs.



Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Certificat
Predefined Rule	Any	Internet	TCP https TCP HTTP_and_HTTPS_proxy	Any	Inspect	None	All	All	Outboun

Action

The action is what is done to the traffic. Click in the column to see the options and select one to add to the rule.

- **Inspect** - The traffic is inspected on the blades set in the **Blades** column.
- **Bypass** - The traffic of source and destination traffic in rules that include the bypass action are not decrypted and inspected. You can bypass HTTPS inspection for all Check Point objects. This is recommended for Anti-Bot, Anti-Virus, URL Filtering, and IPS updates. Other HTTPS protections that already operate on traffic will continue to work even when the HTTPS traffic is not decrypted for inspection.

See also, page 35 of R77 Application Control and URL Filtering Administration Guide (quote shown as indented text below):

You can enable HTTPS traffic inspection on Security Gateways to inspect traffic that is encrypted by the Secure Sockets Layer (SSL) protocol.

See also, page 35 of R77 Application Control and URL Filtering Administration Guide (quote shown as indented text below):

There are two types of HTTPS inspection:

- **Inbound HTTPS inspection** - To protect internal servers from malicious requests originating from the internet or an external network.
- **Outbound HTTPS inspection** - To protect an organization from malicious traffic being sent by an internal client to a destination outside of the organization.

How it operates

In outbound HTTPS inspection, when a client in the organization initiates an HTTPS connection to a secure site, the Security Gateway:

1. Intercepts the request.
2. Establishes a secure connection to the requested web site and validates the site server certificate.
3. Creates a new SSL certificate for the communication between the Security Gateway and the client, sends the

	client the new certificate and continues the SSL negotiation with it. 4. Using the two SSL connections: a. It decrypts the encrypted data from the client. b. Inspects the clear text content for all blades set in the Policy. c. Encrypts the data again to keep client privacy as the data travels to the destination web server resource. In inbound HTTPS inspection, when a client outside of the organization initiates an HTTPS connection to a server behind the organization's gateway, the Security Gateway: 1. Intercepts the request. 2. Uses the server's original certificate and private key to initiate an SSL connection with the client. 3. Creates and establishes a new SSL connection with the web server. 4. Using the two SSL connections: a. It decrypts the encrypted data from the client. b. Inspects the clear text content for all blades set in the policy. c. Encrypts the data again to keep client privacy as the data travels to the destination server behind the gateway. See also, page 36 of R77 Application Control and URL Filtering Administration Guide (quote shown as indented text below): You must enable HTTPS inspection on each Security Gateway. From **Security Gateway > HTTPS Inspection > Step 3** > Select **Enable HTTPS Inspection**. Thus, the Check Point R77 system operates a method that includes identifying encrypted data, and in doing so satisfies the requirements of claim element 1c.
1d. determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising	The Check Point R77 system performs determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators. Exponent showed in the analysis of claim element 1a that the Check Point R77 is capable of performing domain-specific blocking for HTTP files. Although some of the packets involved in HTTPS communication contain encrypted data, the domain

encrypted data that corresponds to the one or more network-threat indicators;	name can be transmitted as unencrypted data, as is shown in the handshake data packet in Figure 21.

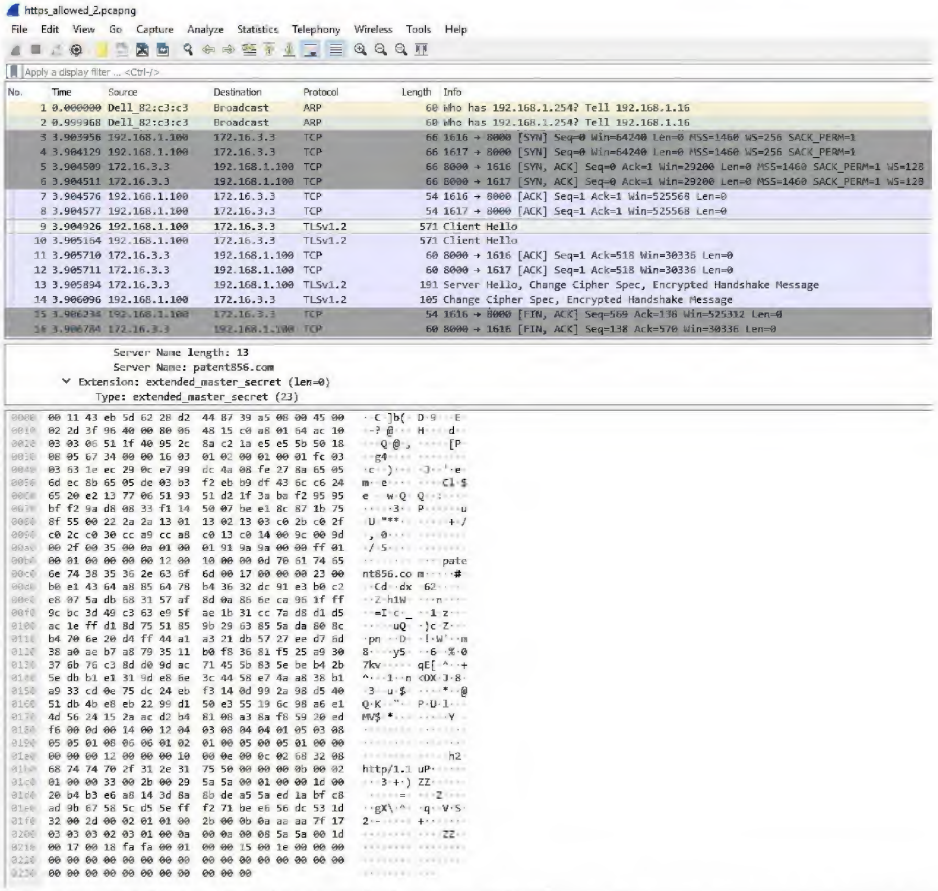


Figure 21: "Client Hello" packet during https handshake, showing "Patent856.com" as an unencrypted segment in the packet (lines 00c0 and 00d0).

CENTRIPETAL-CSCO 088036

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 536

	Futhermore, additional information such as the IP packet header information is also unencrypted data. Therefore, the method employed by the Check Point R77 system of determining "packets comprising encrypted data that corresponds to the one or more network-threat indicators" is based on unencrypted data.
1e. filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and	The Check Point R77 system performs filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators. The analysis of claim element 1a showed that the R77 system is capable of performing URI-specific blocking, in which setting a block for http://patent856.com prevented access to the site but access to http://patent857.com was permitted. Thus, Exponent has shown that the Check Point R77 system operates a method wherein the packet-filtering system filters packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators based on a URI specified by a packet-filtering rule. In addition to this testing, the documentation for the Check Point R77 system also indicates this functionality. For example, see page 39 of the R77 Application Control and URL Filtering Administration Guide. This describes how the HTTPS Inspection Policy performs traffic inspection (quote shown as indented text below): > The HTTPS inspection policy determines which traffic is inspected. The primary component of the policy is the Rule Base. The rules use the categories defined in the Application and URL Filtering Database, network objects and custom objects (if defined). See also, page 40 of the R77 Application Control and URL Filtering Administration Guide, Predefined Rule, which outlines how predefined rules can be used to inspect and filter traffic (quote shown as indented text below):

	Predefined Rule When you enable HTTPS inspection, a predefined rule is added to the HTTPS Rule Base. This rule defines that all HTTPS and HTTPS proxy traffic from any source to the internet is inspected on all blades enabled in the Blade column. By default, there are no logs.  Page 40 of the R77 Application Control and URL Filtering Administration Guide, regarding services, provides further description of how HTTPS packets are inspected (quote shown as indented text below): By default, HTTPS traffic on port 443 and HTTP and HTTPS proxy on port 8080 is inspected. You can include more services and ports in the inspection by adding them to the services list. To select other HTTPS/HTTP services, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of services and select a service. Other services, such as SSH are not supported. Therefore, the Check Point R77 system filters "packets comprising the portion of the unencrypted data" based upon the packets' URI, which satisfies claim element 1e's requirement that the filtering is based on "at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules."
1f. the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	The Check Point R77 system performs filtering packets comprising the encrypted data that corresponds to the one or more network-threat indicators. It was demonstrated in claim 1a that the packets related to domain "patent856.com" were filtered by Check Point R77. In addition to Exponent's testing, documentation for the R77 system describes this functionality. For example, page 35 of R77 Application Control and URL Filtering Administration Guide describes the process of HTTPS inspection (quote shown as indented text below):

Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Certificate
Predefined Rule	Any	Internet	https HTTP_and_HTTPS_proxy	Any	Inspect	None	All	All	Outbound Certificate

	How it operates In outbound HTTPS inspection, when a client in the organization initiates an HTTPS connection to a secure site, the Security Gateway: 1. Intercepts the request. 2. Establishes a secure connection to the requested web site and validates the site server certificate. 3. Creates a new SSL certificate for the communication between the Security Gateway and the client, sends the client the new certificate and continues the SSL negotiation with it. 4. Using the two SSL connections: a. It decrypts the encrypted data from the client. b. Inspects the clear text content for all blades set in the Policy. c. Encrypts the data again to keep client privacy as the data travels to the destination web server resource. In inbound HTTPS inspection, when a client outside of the organization initiates an HTTPS connection to a server behind the organization's gateway, the Security Gateway: 1. Intercepts the request. 2. Uses the server's original certificate and private key to initiate an SSL connection with the client. 3. Creates and establishes a new SSL connection with the web server. 4. Using the two SSL connections: a. It decrypts the encrypted data from the client. b. Inspects the clear text content for all blades set in the policy. c. Encrypts the data again to keep client privacy as the data travels to the destination server behind the gateway. Hence, the Check Point R77 documentation includes descriptions of how the policy defined by the Check Point R77 system can be used to determine how encrypted packets are filtered.
1g. routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.	The Check Point R77 system performs routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators. Documentation for the Check Point R77 system describes this functionality. Specifically, page 55 of Check Point IPS Administration Guide R77 ("Working with Packet Information") describes how packet capture is possible (quote shown as indented text below): **Capturing a Packet for Every Log** To capture packet data for a protection for every malicious packet that is logged, turn on the packet capture option in that protection. This attaches a packet capture to every log generated by the protection.

	In the middle manual also said that it can log every packet, but default is just log the first packet. We have the option to switch it. **Viewing Packet Capture Data in SmartView Tracker** A packet capture is automatically attached to the first packet logged by a protection since policy installation. If packet capture is turned on for a protection, a packet capture is attached to *every* log generated by the protection. **To view packet captures in SmartView Tracker** From the protection page that has **Capture Packets** selected, click **View Logs.** SmartView Tracker opens. Wait until the log window for the specific protection opens. Note - SmartView Tracker displays the current log file. If you have performed a log switch and the capture is in a different file, open that log file instead. Hence, the Check Point R77 system operates a method in which the packet-filtering system routes filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

Claim 18 Analysis

Claim 18	Analysis of Check Point R77
18a. The method of claim 1, wherein the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client	The Check Point R77 system performs the method of claim 1, wherein the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server. The HTTPS communications observed during this testing detailed in relation to claim elements 1a and 1b include a TLS handshake to setup the encrypted channel. The Wireshark screenshot in Figure 16 shows the handshake and subsequent transfer of data from the client to the server.

CENTRIPETAL-CSCO 088040

Patent Owner, Centripetal Networks, Inc. - Ex. 2022, p. 540

and a server, the method further comprising:	
18b. determining that the one or more handshake messages comprise the domain name identified as the network threat.	The Check Point R77 system performs determining that the one or more handshake messages comprise the domain name identified as the network threat. Claim 1f shows that the domain name is visible in the handshake message. This domain name can be identified as the network threat.

Claim 24 Analysis

Claim 24	Analysis of Check Point R77
24a. A packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;	The Check Point R77 system includes a packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat. See analysis of claim element 1a.

24b. identify packets comprising unencrypted data;	The Check Point R77 system identifies packets comprising unencrypted data. See analysis of claim element 1b.
24c. identify packets comprising encrypted data;	The Check Point R77 system identifies packets comprising encrypted data. See analysis of claim element 1c.
24d. determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;	The Check Point R77 system determines, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators; See analysis of claim element 1d.
24e. filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a	The Check Point R77 system filters, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators. See analysis of claim element 1e.

command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and	
24f. the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	The Check Point R77 system filters the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators. See analysis of claim element 1f.
24g. route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.	The Check Point R77 system routes, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators. See analysis of claim element 1g.

Claim 25 Analysis

Claim 25	Analysis of Check Point R77
25a. One or more non-transitory computer-readable media comprising	The Check Point R77 system includes one or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to: receive data indicating a plurality of network-threat

instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;	indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat. The Check Point R77 system includes non-transitory computer-readable media. See analysis of claim element 1a.
25b. identify packets comprising unencrypted data;	The Check Point R77 system includes non-transitory computer-readable media and identifies packets comprising unencrypted data. See analysis of claim element 1b.
25c. identify packets comprising encrypted data;	The Check Point R77 system includes non-transitory computer-readable media and identifies packets comprising encrypted data. See analysis of claim element 1c.
25d. determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;	The Check Point R77 system includes non-transitory computer-readable media and determines based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators. See analysis of claim element 1d.
25e. filter, by the packet-	The Check Point R77 system includes non-transitory computer-readable media and filters, by the

filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and	packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators. See analysis of claim element 1e.
25f. the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	The Check Point R77 system includes non-transitory computer-readable media and filters the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators. See analysis of claim element 1f.

25g. route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.	The Check Point R77 system includes non-transitory computer-readable media and routes, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators. See analysis of claim element 1g.