Adam Sorini

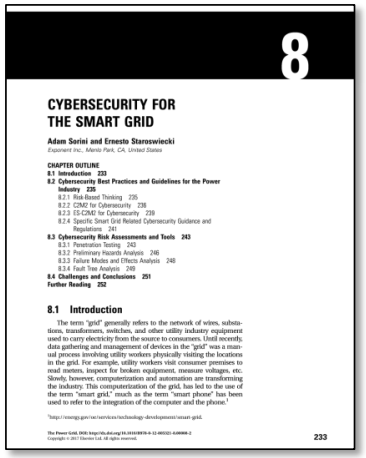
Direct Examination

DDX 2

Dr. Adam Sorini, Ph.D.



Dr. Adam Sorini
B.S., M.S., Ph.D. in Physics



8

CYBERSECURITY FOR THE SMART GRID

Adam Sorini and Ernesto Staroswiecki
Exponent Inc., Menlo Park, CA, United States

CHAPTER OUTLINE
8.1 Introduction 233
8.2 Cybersecurity Best Practices and Guidelines for the Power Industry 235
8.2.1 Risk-Based Thinking 235
8.2.2 C2M2 for Cybersecurity 238
8.2.3 ES-C2M2 for Cybersecurity 239
8.2.4 Specific Smart Grid Related Cybersecurity Guidance and Regulations 241
8.3 Cybersecurity Risk Assessments and Tools 243
8.3.1 Penetration Testing 243
8.3.2 Preliminary Hazards Analysis 246
8.3.3 Failure Modes and Effects Analysis 248
8.3.4 Fault Tree Analysis 249
8.4 Challenges and Conclusions 251
Further Reading 252

8.1 Introduction

The term "grid" generally refers to the network of wires, substations, transformers, switches, and other utility industry equipment used to carry electricity from the source to consumers. Until recently, data gathering and management of devices in the "grid" was a manual process involving utility workers physically visiting the locations in the grid. For example, utility workers visit consumer premises to read meters, inspect for broken equipment, measure voltages, etc. Slowly, however, computerization and automation are transforming the industry. This computerization of the grid, has led to the use of the term "smart grid," much as the term "smart phone" has been used to refer to the integration of the computer and the phone.[1]

[1] http://energy.gov/oe/services/technology-development/smart-grid.

The Power Grid. DOI: http://dx.doi.org/10.1016/B978-0-12-410321-6.00008-2
Copyright © 2017 Elsevier Ltd. All rights reserved.

233

- Senior Managing Scientist at Exponent, an engineering and scientific consulting firm.
- Six-plus years experience in Exponent's Electrical Engineering and Computer Science (EECS) practice.
- 10-15 computer security projects undertaken and resolved.
- 15-20 source code analysis projects undertaken and completed.
- Certified Cyber-Forensics Professional (CCFP) , as recognized by the International Information System Security Certification Consortium.
- Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).
- Author or co-author of several peer-reviewed cybersecurity articles and publications.
- Held Q-Access Security Clearance from the U.S. Department of Energy.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 2

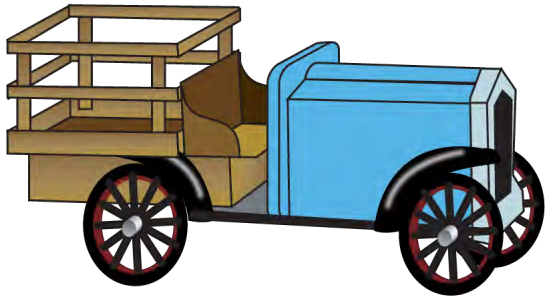
Prior Art Evaluation

- Examined and analyzed written documents
- Ran the software
- Examined user's guides, manuals, datasheets, and other written documentation.
- Set up experiments to better understand specific features, *e.g.,* blocking packets
- Overall, ran numerous experiments and documented the operation of the software

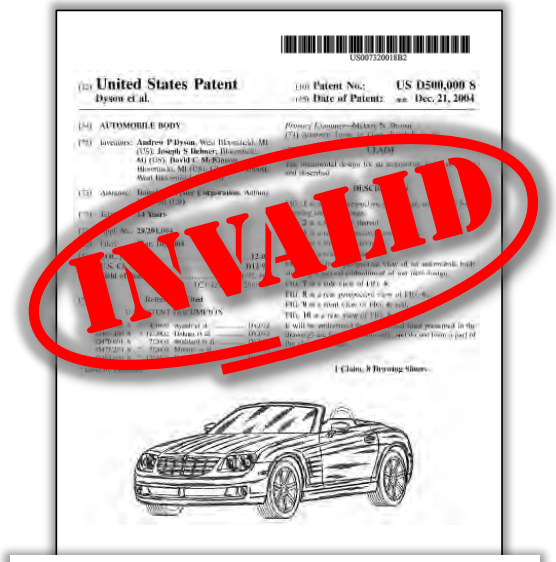
Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 3

Anticipation

Prior Art



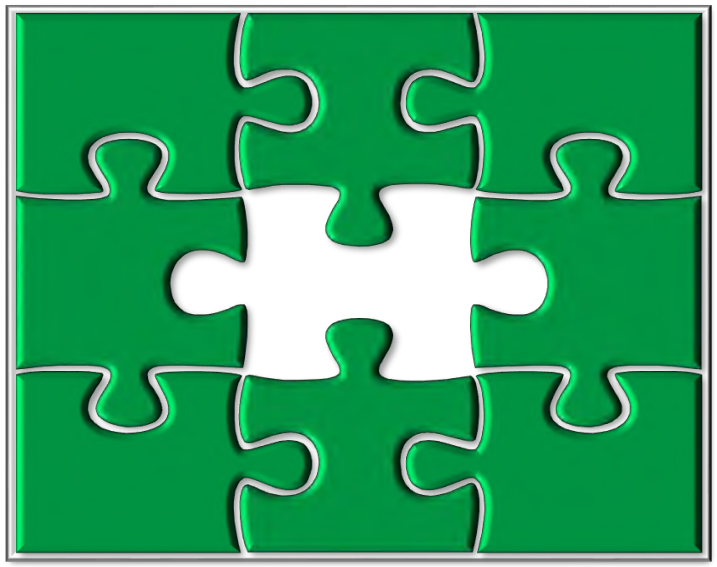
1. A car with:
   - 4 wheels
   - an engine
   - brakes



1. A car with:
   - 4 wheels
   - an engine
   - brakes

Obviousness

- Is the invention obvious to a person of skill in the art at the time of the patent?



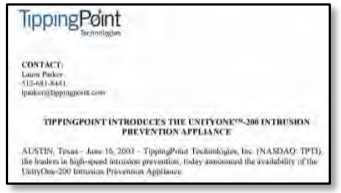


TippingPoint IPS *(Prior Art)*

TippingPoint Technologies

Jun. 16, 2003

TippingPoint Press Release


TippingPoint Technologies

CONTACT:

TIPPINGPOINT INTRODUCES THE UNITYONE™-200 INTRUSION PREVENTION APPLIANCE

DTX641 at p. 48, 49

Oct. 3, 2003

TippingPoint Data Sheet


UnityOne TippingPoint Technologies

DTX641 at p. 49, 52

Dec. 7, 2003

TippingPoint Data Sheet


TippingPoint UnityOne™ Intrusion Prevention Appliances

DTX641 at p. 57, 58

Jan. 25, 2008

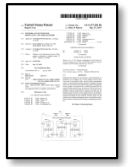
TippingPoint Appliance



DTX590

Oct. 22, 2012

'205 Patent



JTX001

Apr. 16, 2014

'213 Patent



JTX005

2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014

Check Point R75 *(Prior Art)*

Check Point SOFTWARE TECHNOLOGIES LTD.

2010

Copyright ©



DTX592

Dec. 2010

Check Point R75 Release Map



DTX384

Dec. 15, 2010

Check Point R75 Product Documentation



DTX386

Jan. 2, 2011

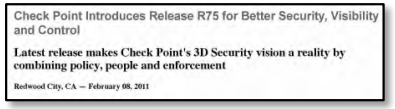
Check Point R75 YouTube Video



DTX455

Feb. 8, 2011

Check Point R75 Press Release


Check Point Introduces Release R75 for Better Security, Visibility and Control

Latest release makes Check Point's 3D Security vision a reality by combining policy, people and enforcement

Redwood City, CA — February 08, 2011

DTX641 at p.6, 8

Feb. 13, 2011

Check Point R75 Press Release



DTX641 at p.2

Oct. 22, 2012

'205 Patent



JTX001

Apr. 16, 2014

'213 Patent



JTX005

2009 | 2010 | 2011 | 2012 | 2013 | 2014

Check Point R77 *(Prior Art)*

Check Point SOFTWARE TECHNOLOGIES LTD.

Aug. 26-27, 2013

Check Point R77 Product Documentation



DTX388, DTX017, DTX018

2014

Copyright ©



DTX593

Sep. 2, 2014

Third Party Review of Check Point R77



DTX433

Jul. 2014

Check Point R77 Release Map



DTX384

Jul. 15, 2014

Check Point R77 Website



DTX641

Apr. 17, 2015

'722 Patent



JTX003

Dec. 23, 2015

'856 Patent



JTX006

2013 | 2014 | 2015

PoliWall™ *(Prior Art)*

PoliWall™

2006

First PoliWall with HIPPIE used



Maestras Depo. 27:7-14

Sep. 2010

PoliWall Manual ver. 2.00.01



DTX156

Jan. 2011

PoliWall Manual ver. 2.01.01



DTX157

Jan. 13, 2011

PoliWall sales

DTX163



Mar. 3, 2011

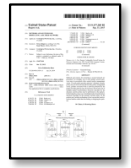
PoliWall YouTube demonstration



DTX158

Oct. 22, 2012

'205 Patent



JTX001

Apr. 17, 2015

'722 Patent



JTX003

2006	2007	2008	2009	2010	2011	2012	2013	2014	2015

Anue 5236 Net Tool Optimizer *(Prior Art)*

Anue 5236 Net Tool Optimizer

3/3/09

Sale of NTO 5236 to Allstate



DTX473

Mar. - Dec. 2009

Over a dozen sales of NTO 5236



DTX466

Aug. 27, 2009

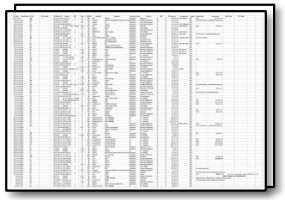
NTO 5236 User's Guide



DTX473

Jan. - Dec. 2010

Dozens of sales of NTO 5236



DTX467

Jan. – Dec. 2011

Dozens more sales of NTO 5236



DTX468

Oct. 22, 2012

'077 Patent

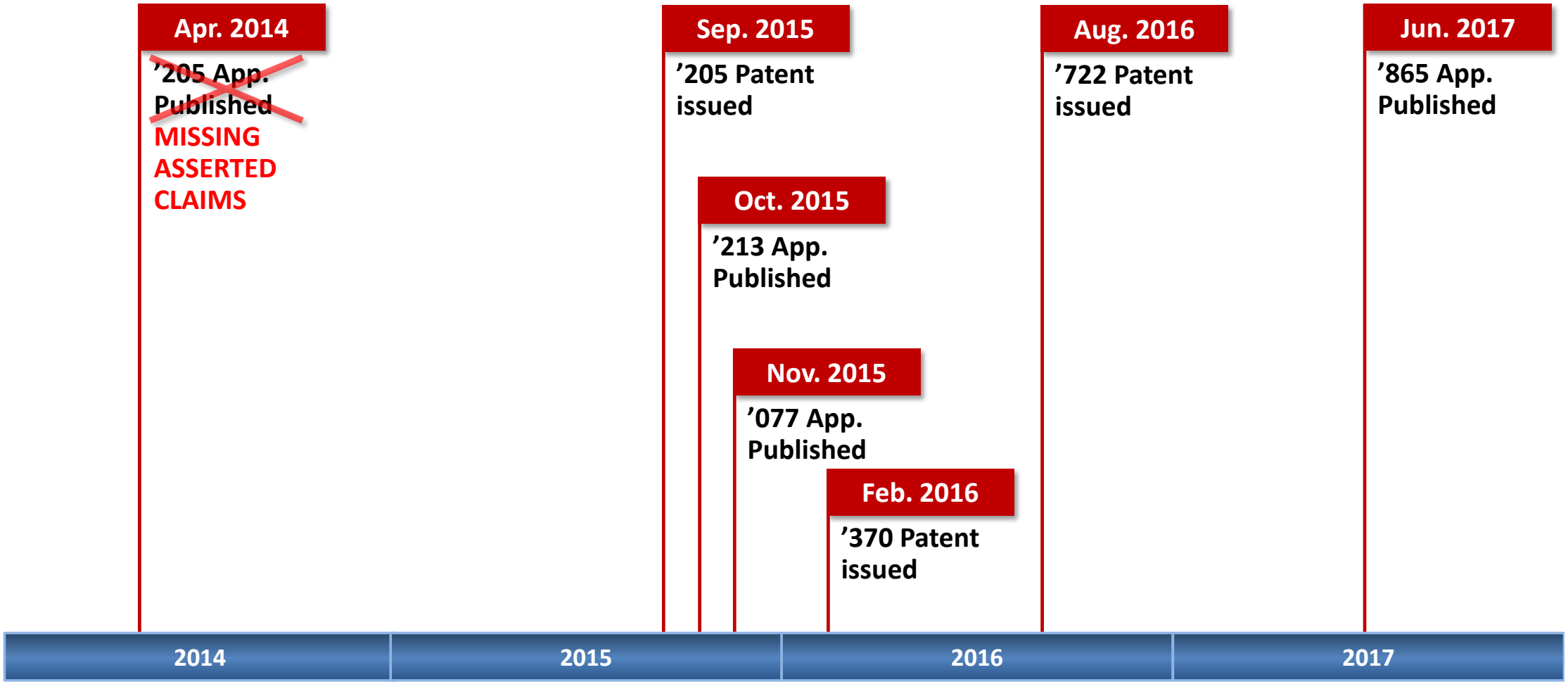


JTX004

2009 | 2010 | 2011 | 2012

Code Counting

First Disclosure of Asserted Claims



Normalization Charts

3-8 Sizing **SEER for Software Detailed Reference**

Source Language	Target Language							
	3GL	4GL	C	C++	COBOL	Java	SQL	Assembly
3GL	1.00	0.56	1.10	1.34	1.23	0.94	0.46	7.48
4GL	1.78	1.00	1.97	2.38	2.19	1.68	0.81	13.32
C	0.91	0.51	1.00	1.21	1.11	0.86	0.41	6.78
C++	0.75	0.42	0.83	1.00	0.92	0.71	0.34	5.60
COBOL	0.81	0.46	0.90	1.09	1.00	0.77	0.37	6.09
Java	1.06	0.59	1.17	1.41	1.30	1.00	0.48	7.92
SQL	2.19	1.23	2.41	2.92	2.69	2.06	1.00	16.35
Assembly	0.13	0.08	0.15	0.18	0.16	0.13	0.06	1.00

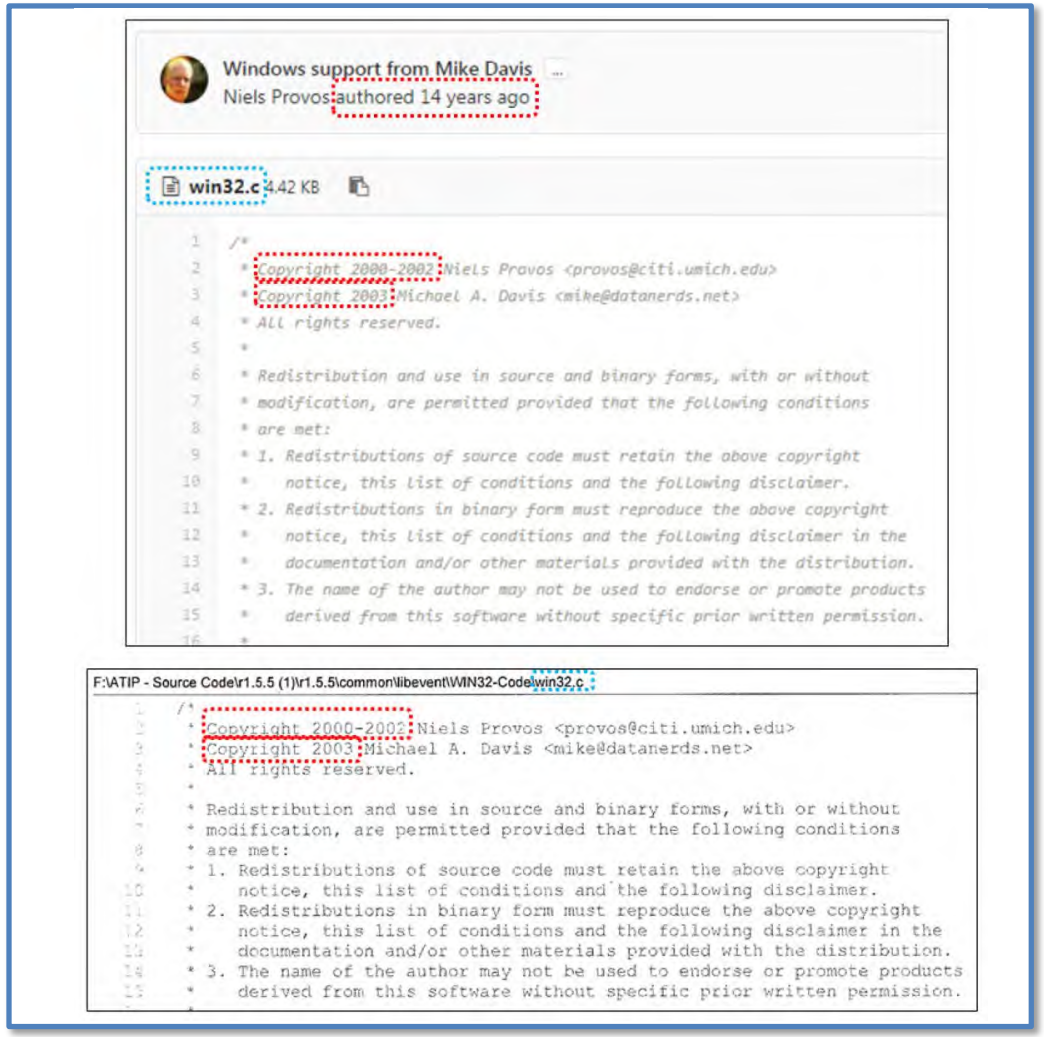
General Language Conversion Factors

Large tasks – Line count ratio

Larger numbers indicate that the language on the top needs longer code	C	C++	Fortran	Java	Common Lisp	Python	C sharp	JavaScript	R	MATLAB	Clojure	Pascal	Haskell	Ruby
Mathematica	17.	9.1	8.1	6.4	6.3	7.2	6.4	5.	3.2	3.2	1.6	5.8	3.5	5.2
Ruby	2.7	1.8	1.9	1.3	1.1	1.1	1.5	0.96	0.72	0.94	0.39	1.4	0.7	
Haskell	3.6	2.7	2.5	2.	1.6	1.7	2.2	1.5	1.1	1.5	0.67	2.1		
Pascal	2.2	1.5	1.2	0.83	0.77	0.8	1.	0.79	0.46	0.61	0.2			
Clojure	8.8	5.3	5.2	3.6	3.7	3.3	3.8	2.5	1.9	2.9				
MATLAB	3.6	2.4	1.8	1.1	1.4	1.1	1.7	0.94	0.75					
R	4.7	3.3	2.4	1.9	1.8	1.7	2.1	1.5						
JavaScript	2.8	2.1	1.9	1.2	1.2	1.1	1.6							
C sharp	2.	1.4	1.3	0.91	0.8	0.82								
Python	2.2	1.6	1.5	1.1	0.88									
Common Lisp	2.8	1.8	1.6	1.3										
Java	2.1	1.4	1.5											
Fortran	1.4	1.												
C++	1.4													

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 13

Old Public Code



Old Public Code

F:\ATIP - Source Code\r1.5.5 (1)\r1.5.5\common\libevent\WIN32-Code\tree.h

```
/*  $OpenBSD: tree.h,v 1.7 2002/10/17 21:51:54 art Exp $    */
/*
 * Copyright 2002 Niels Provos <provos@citi.umich.edu>
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
```

Old Irrelevant Code

E:\ATI - Source Code\ati-stable\ati-stable\tests\bpsruby\c_ext\nptunnel\packet.c

```
/* $Id$
 *
 * Copyright (c) 2007-2010 BreakingPoint Systems, Inc.  All rights reserved.
 *
 * Unauthorized reproduction is prohibited by law. Patent Pending. No part of
 * this file may be disclosed, distributed, reproduced, stored in a retrieval
 * system or transmitted in any form or by any means, electronic, mechanical,
 * photocopying, recording or otherwise, without the express written permission
 * of BreakingPoint Systems, Inc.
 *
 * $LastChangedBy$
 * $LastChangedDate$
 * $Revision$
 * $HeadURL$
 */

#include <stdlib.h>
#include <string.h>
#include <assert.h>
#include "packet.h"

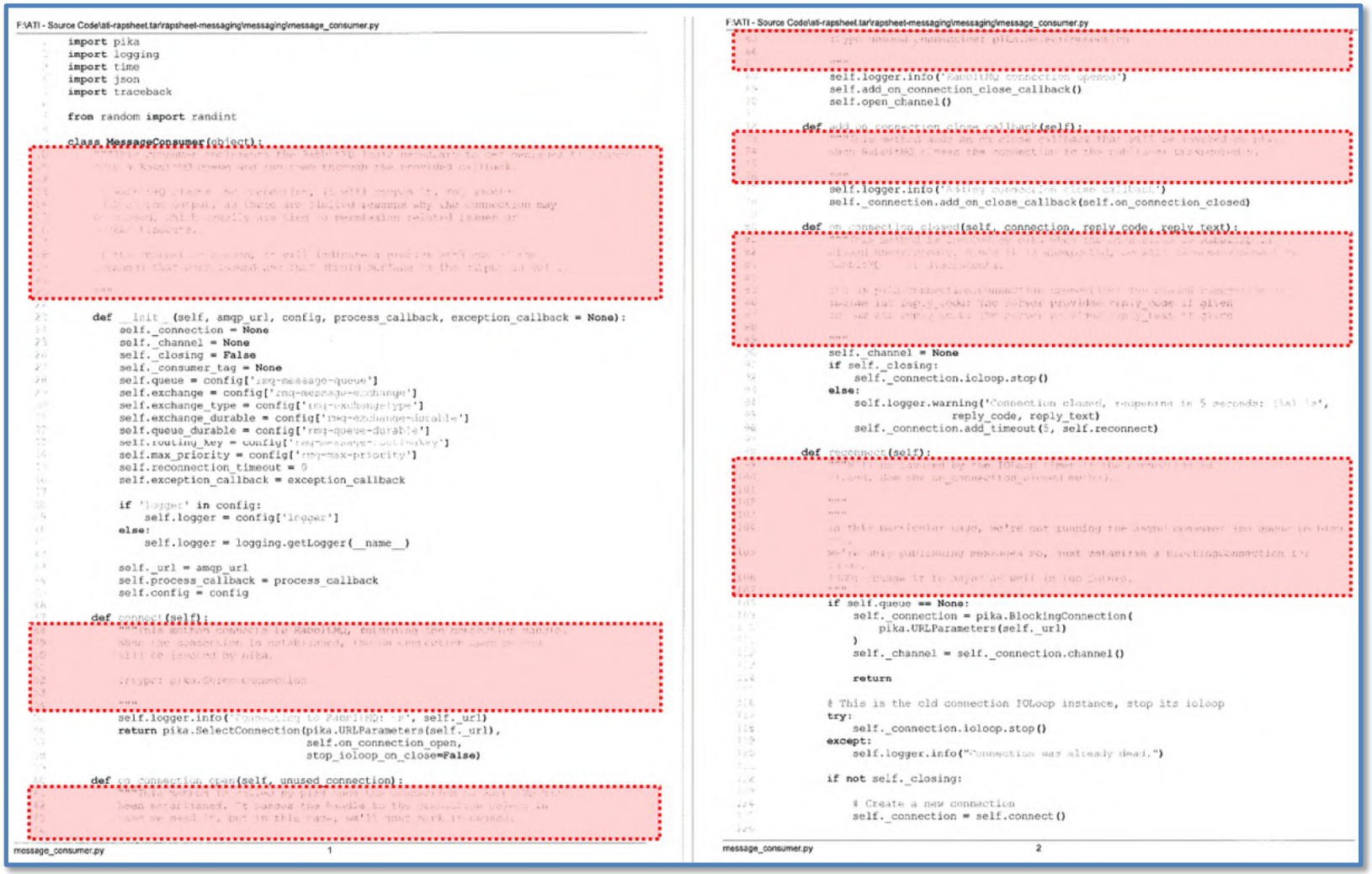
packetlist
packetlist_new()
{
```

Old Google Code

E:\ATI - Source Code\ati-stable\ati-stable\tests\bpsruby\c_ext\aead\curve25519-donna.c

```
/* Copyright 2008, Google Inc.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are
 * met:
 *
 *     * Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *     * Redistributions in binary form must reproduce the above
 * copyright notice, this list of conditions and the following disclaimer
 * in the documentation and/or other materials provided with the
 * distribution.
 *     * Neither the name of Google Inc. nor the names of its
 * contributors may be used to endorse or promote products derived from
 * this software without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
```

Multi-Line Python Comments



MatrixSSL

Exceprt from "corelib.c" (counted by Dr. Goodrich)

F:\ATIP - Source Code\r1.5.5 (1)\r1.5.5\common\matrixssl\core\corelib.c

```
/*
 *  Copyright (c) 2013-2015 INSIDE Secure Corporation
 *  All Rights Reserved
 *
 *  THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF INSIDE
 *
 *  Please do not edit this file without first consulting INSIDE support.
 *  Unauthorized changes to this file are not supported by INSIDE.
 *
 *  The copyright notice above does not evidence any actual or intended
 *  publication of such source code.
 *
 *  This Module contains Proprietary Information of INSIDE and should be
 *  treated as Confidential.
 *
 *  The information in this file is provided for the exclusive use of the
 *  licensees of INSIDE. Such users have the right to use, modify,
 *  and incorporate this code into products for purposes authorized by the
 *  license agreement provided they include this notice and the associated
 *  copyright notice with any such product.
 *
 *  The information in this file is provided "AS IS" without warranty.
 */
#include "coreApi.h"

/*
    Open (initialize) the Core module
    The config param should always be passed as:
        PSCORE_CONFIG
 */
static char g_config[ ] = "N";

int32 psCoreOpen(char *config)
{
    if (*g_config == 'Y') {
        return PS_CORE_IS_OPEN;
    }
    strncpy(g_config, PSCORE_CONFIG, sizeof(g_config) - );
    if (strncmp(g_config, config, sizeof(g_config) - ) != ) {
        psErrorStr( "Core config mismatch.\n" \
            "Library: " PSCORE_CONFIG\
            "\nCurrent: %s\n", config);
        return -;
    }

    if (halOpen() < ) {
        return PS_FAILURE;
    }

    if (osdepTimeOpen() < ) {
        psTraceCore("osdepTimeOpen failed\n");
        return PS_FAILURE;
    }
    if (osdepEntropyOpen() < ) {
```

corelib.c 1

```
/*
 *  Copyright (c) 2013-2015 INSIDE Secure Corporation
 *  All Rights Reserved
```

Vendor utility code "matrixssl" from Github "corelib.c" (numerous logical lines show exact match)

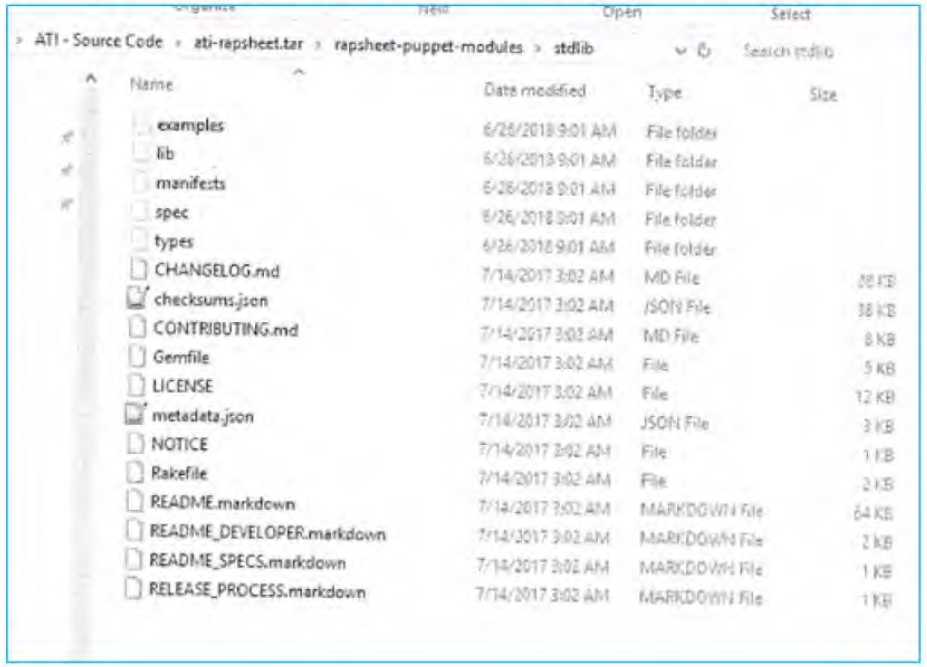
```
/******************************************************************************/
/*
    Open (initialize) the Core module
    The config param should always be passed as:
        PSCORE_CONFIG
 */
static char g_config[32] = "N";

/******************************************************************************/
int32 psCoreOpen(const char *config)
{
    if (*g_config == 'Y')
    {
        return PS_CORE_IS_OPEN;
    }
    strncpy(g_config, PSCORE_CONFIG, sizeof(g_config) - 1);
    if (strncmp(g_config, config, strlen(PSCORE_CONFIG)) != 0)
    {
        psErrorStr( "Core config mismatch.\n" \
            "Library: " PSCORE_CONFIG \
            "\nCurrent: %s\n", config);
        return -1;
    }
```

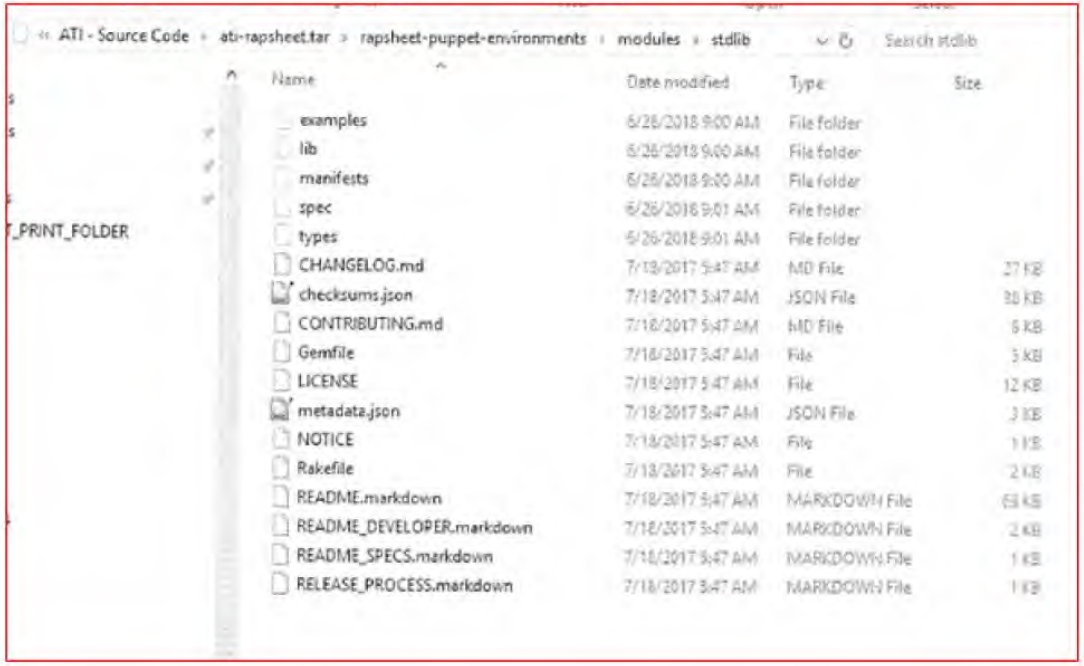
GitHub, Inc. [US] | https://github.com/matrixssl/matrixssl/blob/master/core/corelib.c

Duplicate Code

"ati-rapsheet.tar/rapsheet-puppet-***modules***/stdlib/"



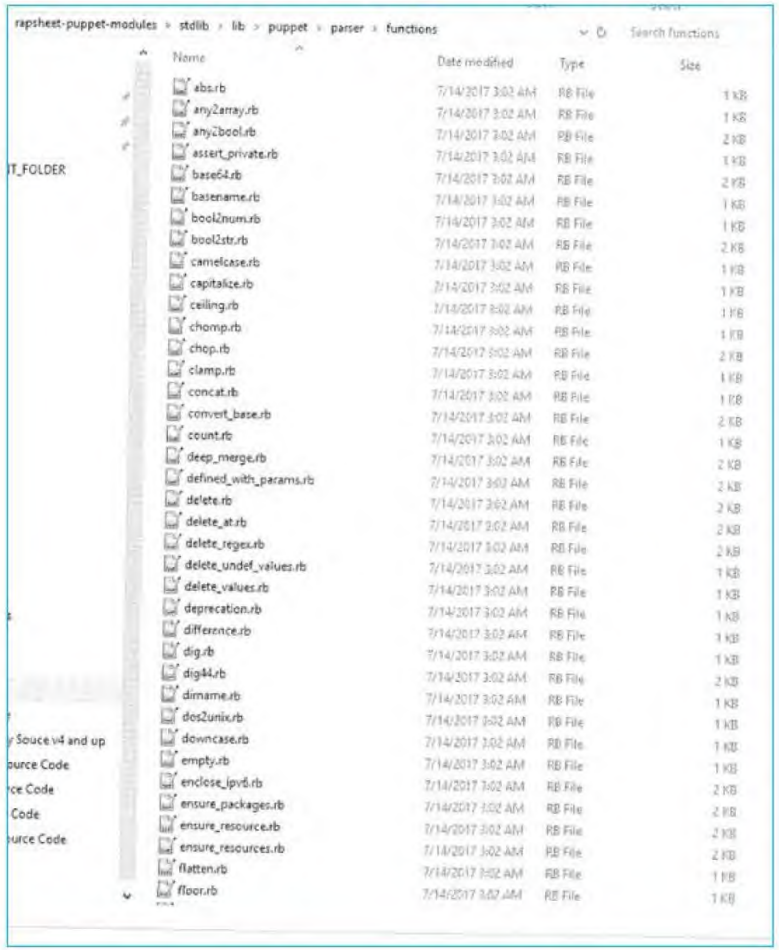
"ati-rapsheet.tar/rapsheet-puppet-***environment***/..."



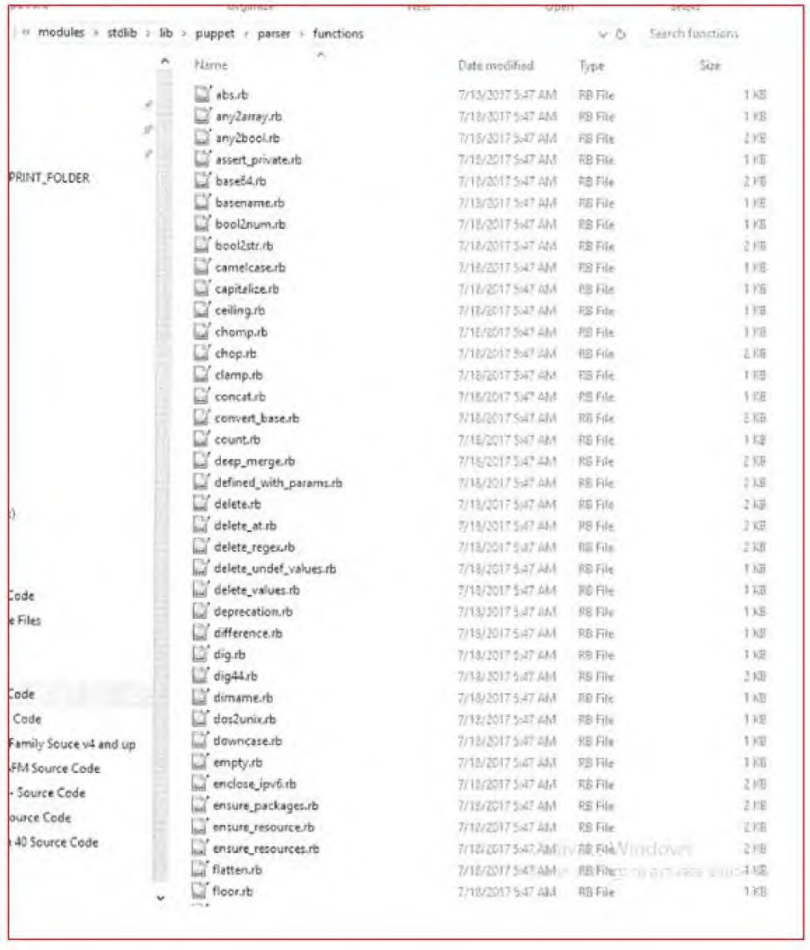
Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 20

Duplicate Code

"ati-rapsheet.tar/rapsheet-puppet-***modules***/stdlib/..."



"ati-rapsheet.tar/rapsheet-puppet-***environment***/..."



Duplicate Code

"ati-rapsheet.tar/rapsheet-puppet-***modules***/stdlib/..."



"ati-rapsheet.tar/rapsheet-puppet-***environment***/..."



Security Requirements

Extra Hi+

Extra Hi-

Very High+

Very High

Very High-

High+

High

High-

Nominal +

Nominal

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 23

Estimated Costs Vary Drastically Depending on Security Requirement

Materials Reviewed

Daniel D. Galorath and Michael W. Evans "Software Sizing, Estimation, and Risk Management" Auerbach Publications, 2006 (ISBN 0-8493-3593-0)



Table 3.3 Approximate Effective Technology Offsets in SEER-SEM[a]

Parameter	Relative Contribution (Percent)	Parameter	Relative Contribution (Percent)
Security requirements	347	Resource dedication	25
Rehost from development to target	93	Process volatility	24
Analyst capabilities	71	Specification level; reliability	22
Programmer capabilities	67	Logon through hardcopy turnaround	22
Time constraints	60	Real time code	21
Practices and methods experience/ process improvement	47	Test level	21
Requirements volatility	47	Host system volatility	19
Product reusability	44	Target system volatility	16
Analyst's application experience/ application class complexity	40	Host development system experience/ complexity	15
Automated tool use	35	Multiple site development	24
Memory constraints	33	Terminal response time	13
Modern development practices	31	Special display requirements	11
Programmer's language experience/ language complexity	30	Target system experience/ complexity	7
Resource and support location	28	QA level	6

Sorini Rebuttal Report at Tables 1 and 3.3

Modified Development Costs

	Development Cost (Labor)	Estimated Schedule for Development (months)
Application Threat Intelligence (C files)	83,961	7.43
Application Threat Intelligence (Ruby files)	91,644,071	76.5
Application Threat Intelligence (Embedded Ruby files)	425,299	12.76
Application Threat Intelligence (Python files)	1,851,618	20.84
Application Threat Intelligence (JavaScript files)	92,828	7.68
TOTAL	94,097,777	

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 25

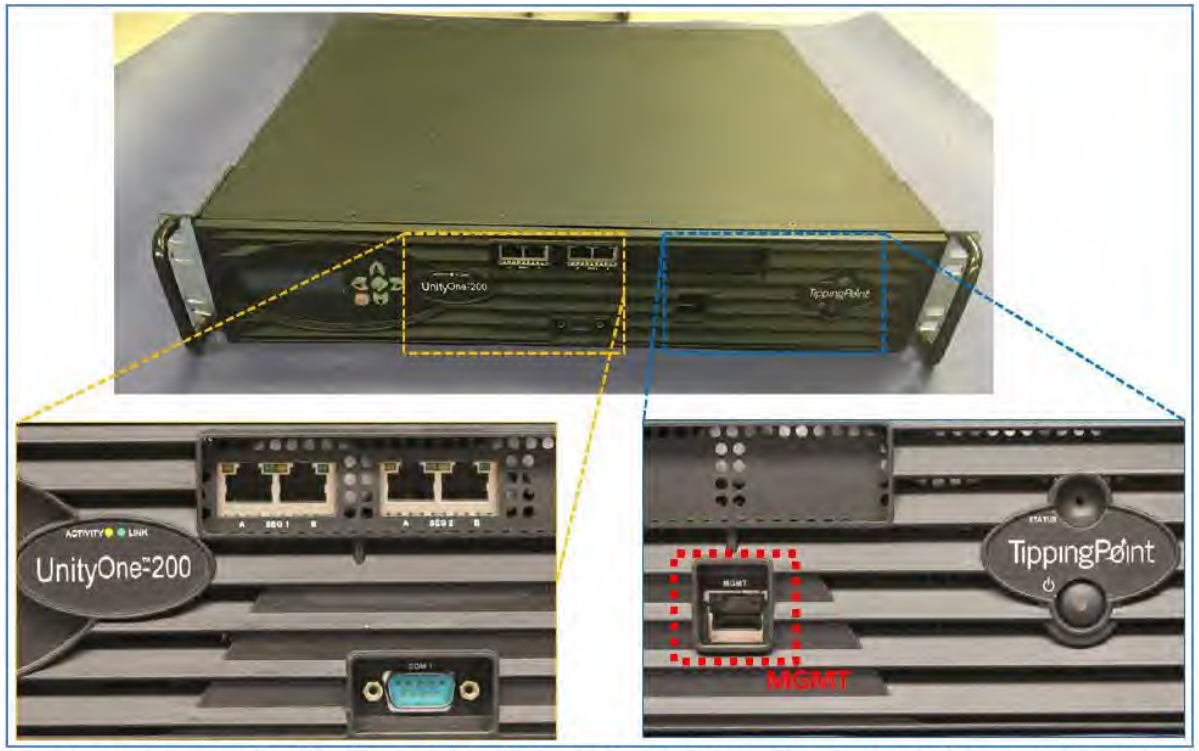
Invalidity

TippingPoint IPS Invalidates the ’205 Patent Claim 17

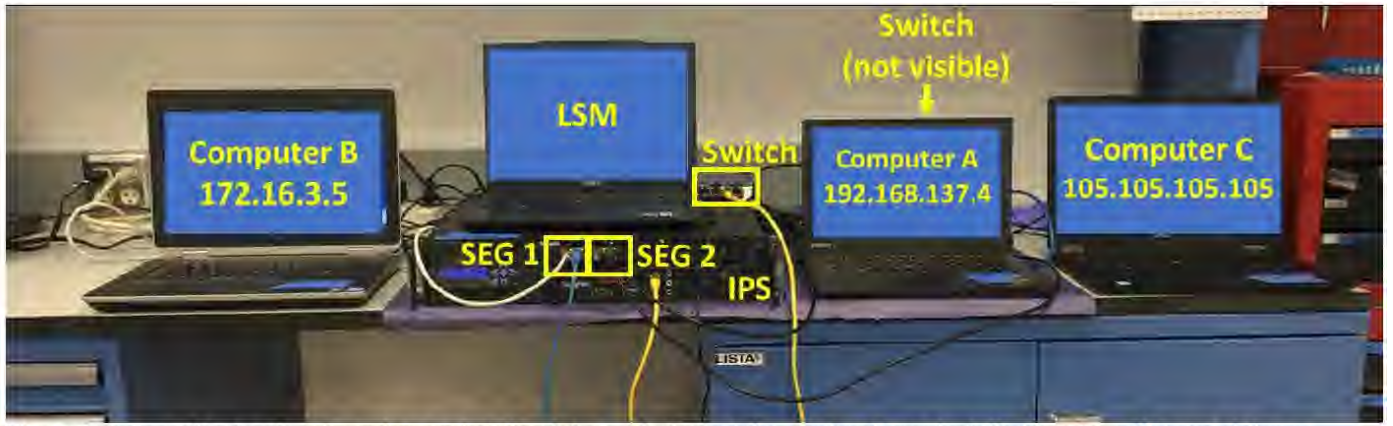
TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. **[a]** 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:	
[b] receive a plurality of dynamic security policies from the security policy management server,	
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

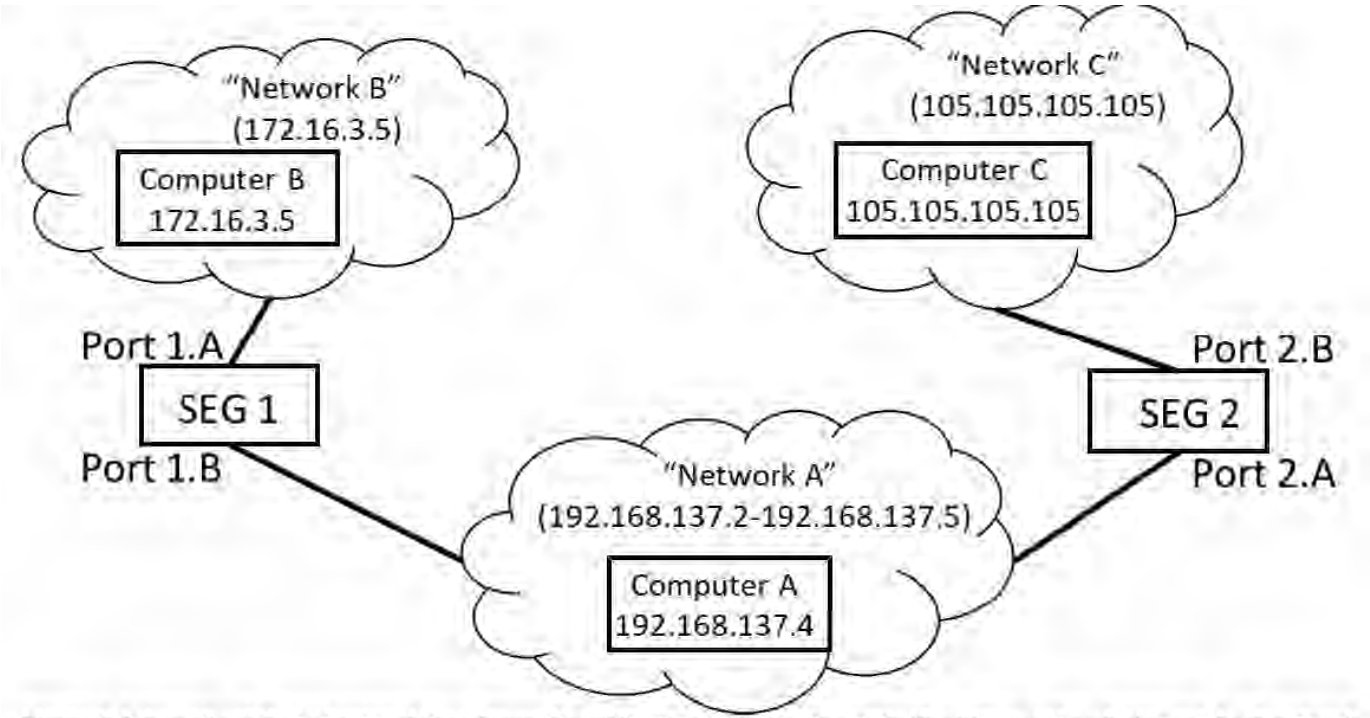
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17. [a] 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:	 **Figure 2: Annotated photographs of the TippingPoint IPS showing two packet security gateway interfaces (lower left) and one management interface (lower right).**

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17. [a] 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:	 **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.**

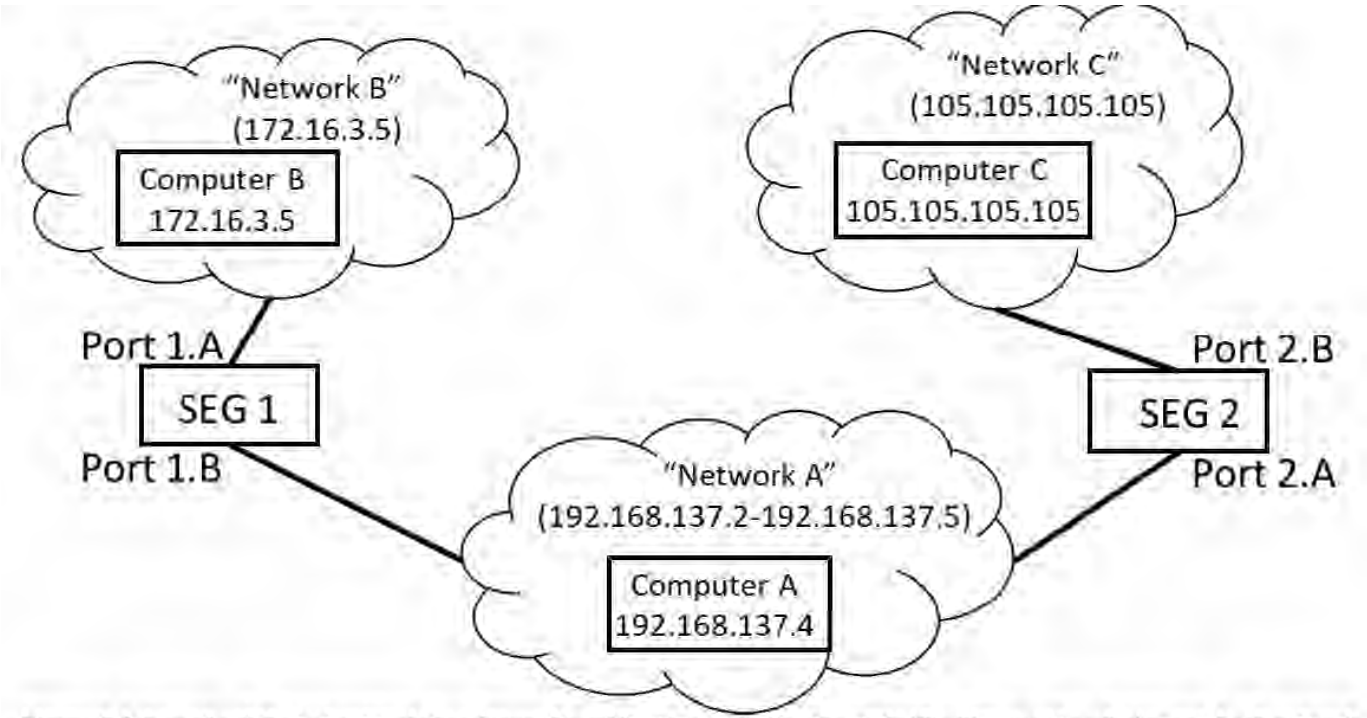
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17. [a] 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:	 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.

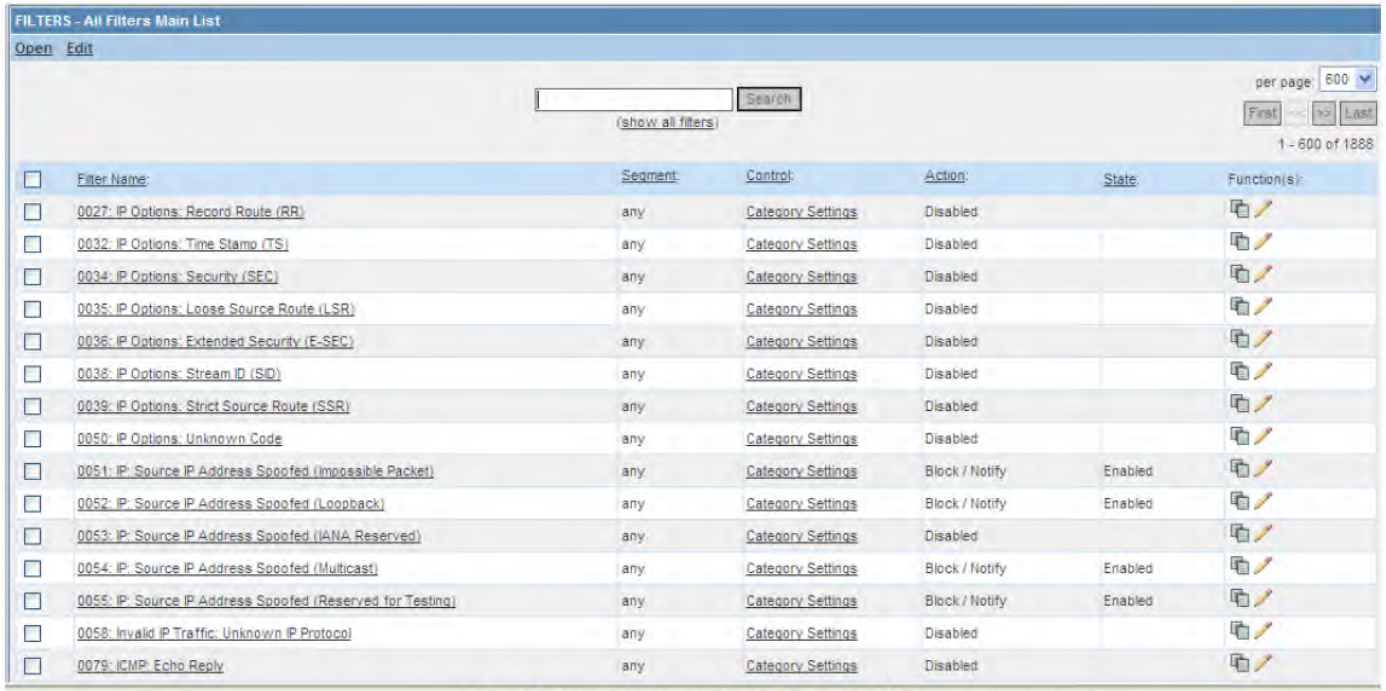
TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	 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.

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	

FILTERS - All Filters Main List

Open Edit

Search

(show all filters)

per page: 600

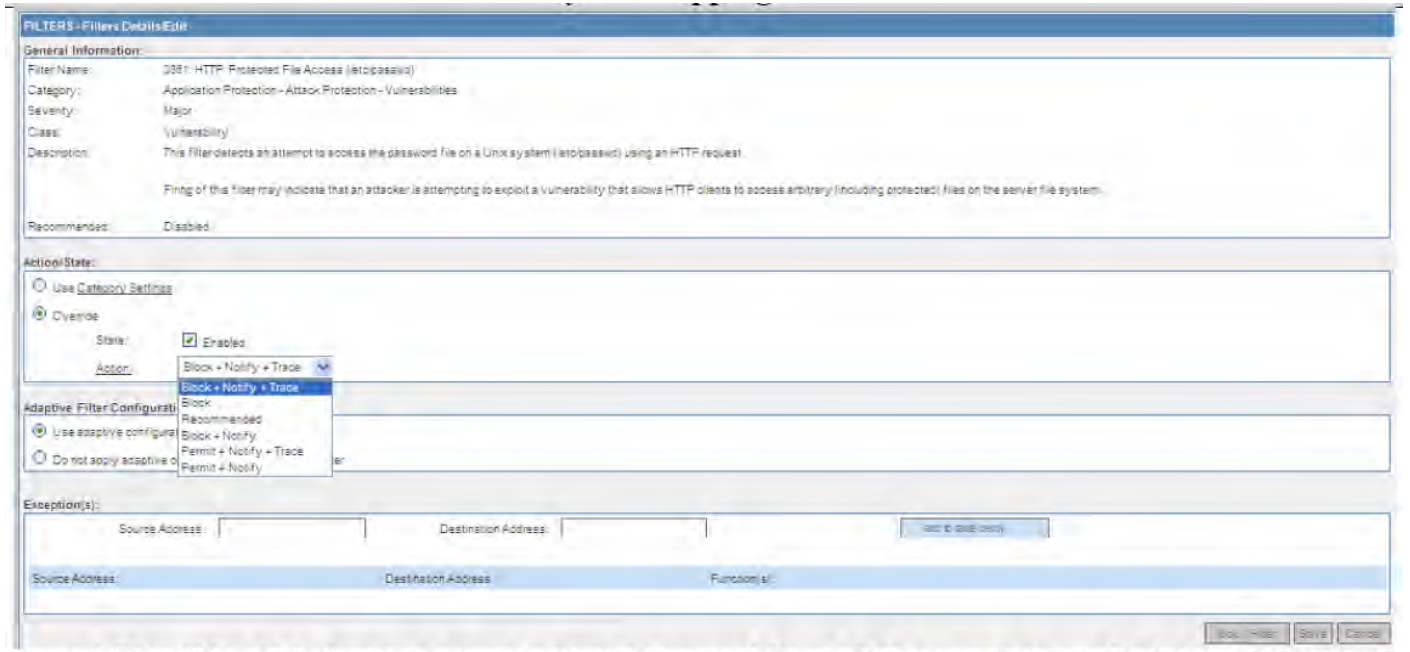
First << >> Last

1 - 600 of 1888

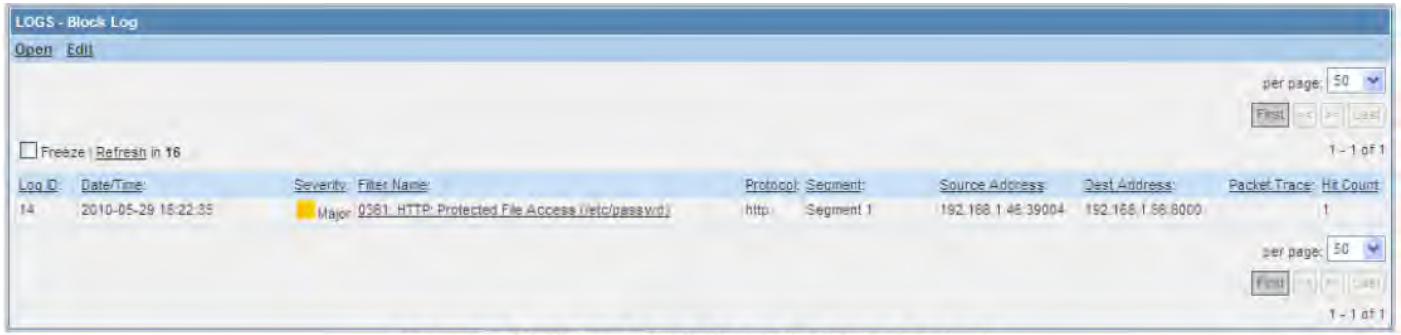
Filter Name:	Segment:	Control:	Action:	State:	Function(s):
0027: IP Options: Record Route (RR)	any	Category Settings	Disabled		
0032: IP Options: Time Stamp (TS)	any	Category Settings	Disabled		
0034: IP Options: Security (SEC)	any	Category Settings	Disabled		
0035: IP Options: Loose Source Route (LSR)	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 5: Sample filters available in the IPS.

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	 **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.**

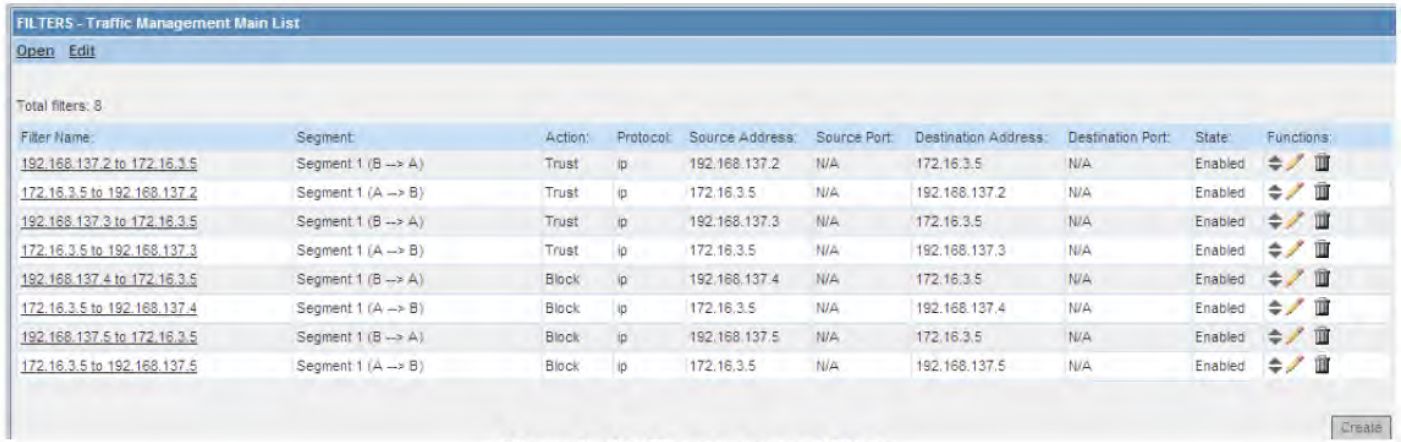
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	 **Figure 7: Block Log, which shows the blocked packets.**

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	 **Figure 8: Alert Log that shows packets that the filter identified but allowed to pass through the gateway.**

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	

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:
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 192.168.137.2	Segment 1 (A --> B)	Trust	ip	172.16.3.5	N/A	192.168.137.2	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 192.168.137.3	Segment 1 (A --> B)	Trust	ip	172.16.3.5	N/A	192.168.137.3	N/A	Enabled	
192.168.137.4 to 172.16.3.5	Segment 1 (B --> A)	Block	ip	192.168.137.4	N/A	172.16.3.5	N/A	Enabled	
172.16.3.5 to 192.168.137.4	Segment 1 (A --> B)	Block	ip	172.16.3.5	N/A	192.168.137.4	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	
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	

Create

Figure 9: Traffic management filters.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 38

’205 Patent Analysis – TippingPoint IPS

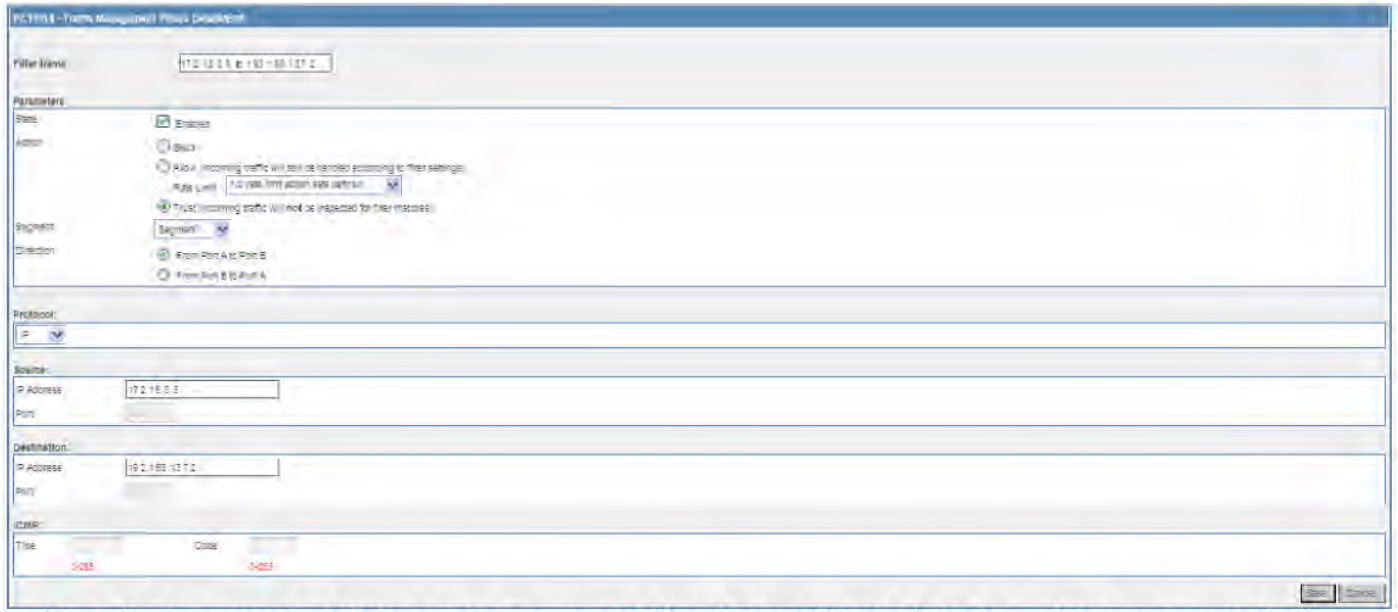
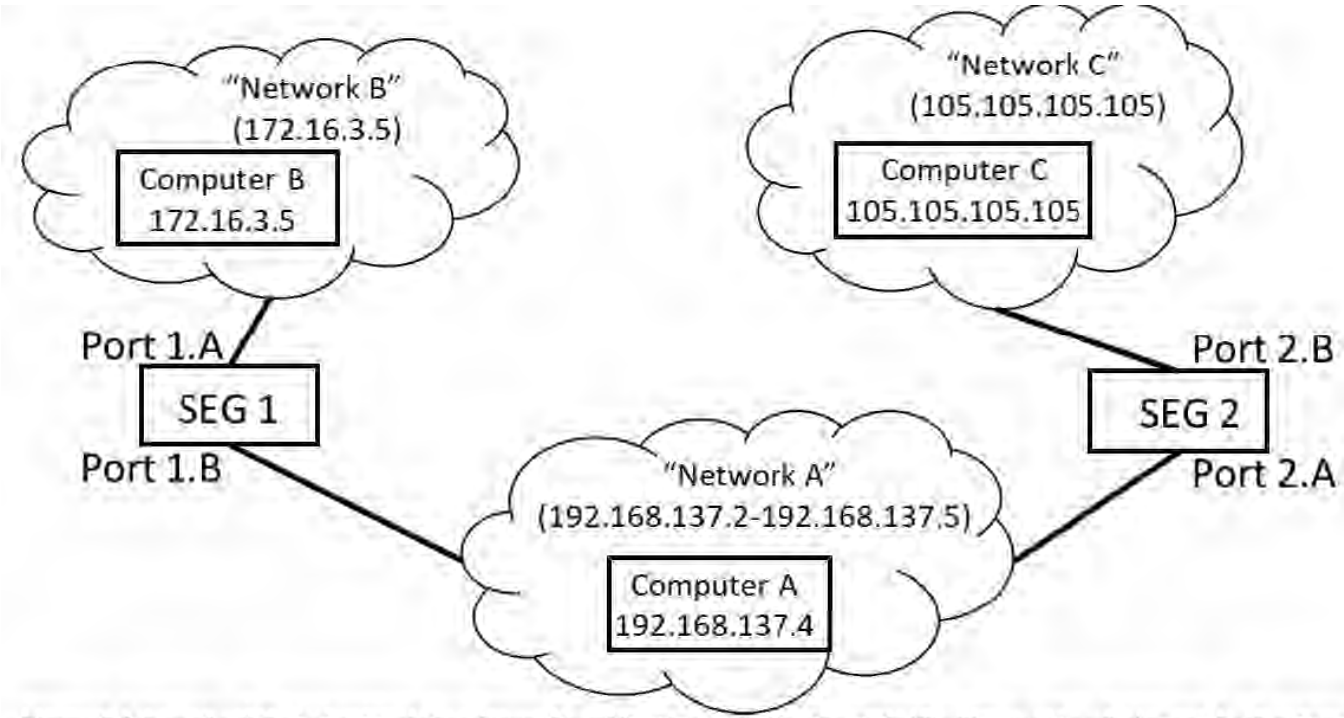
’205 Patent:	TippingPoint:
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	

Figure 10: Parameters for defining a traffic management filter. The “save” button in the lower right corner creates the filter.

TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [c] 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;	 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.

’205 Patent Analysis – TippingPoint IPS

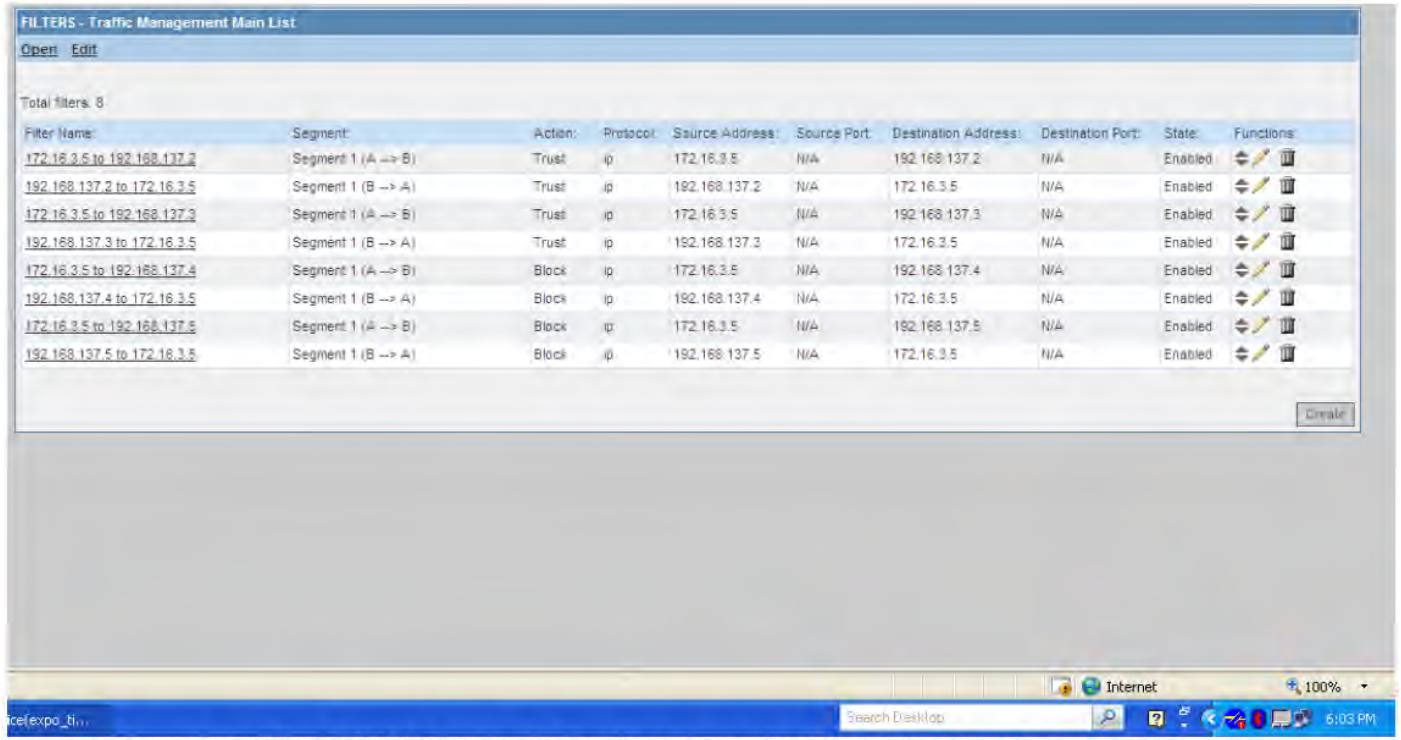
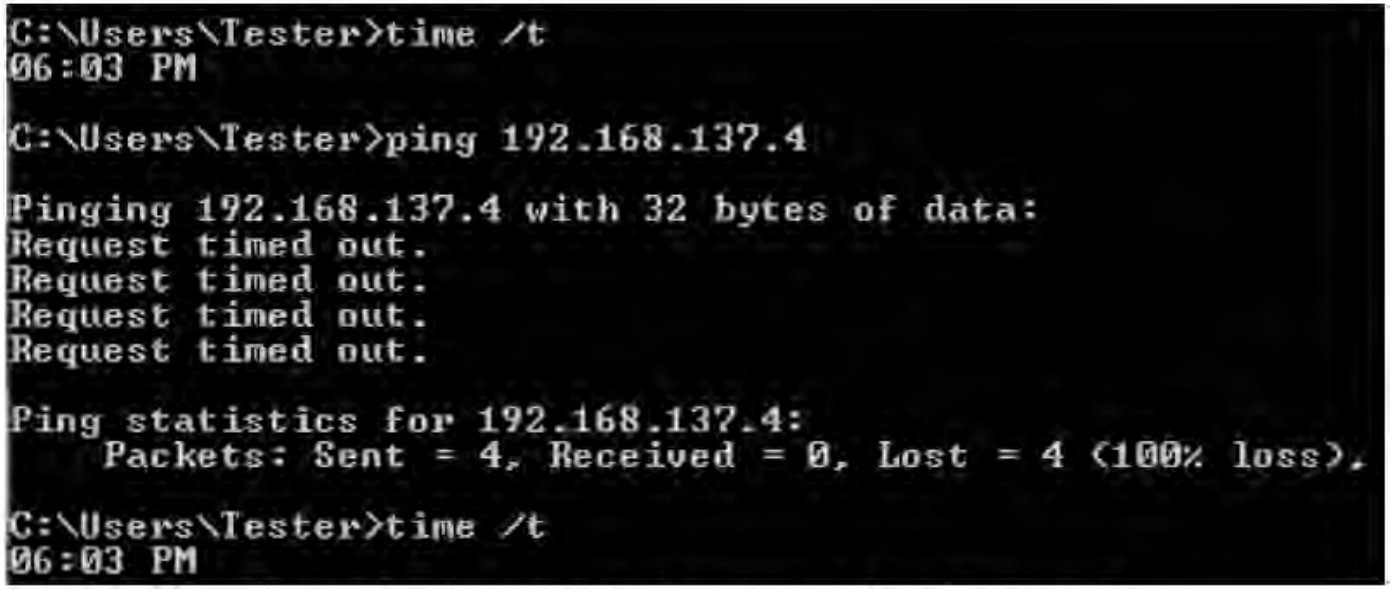
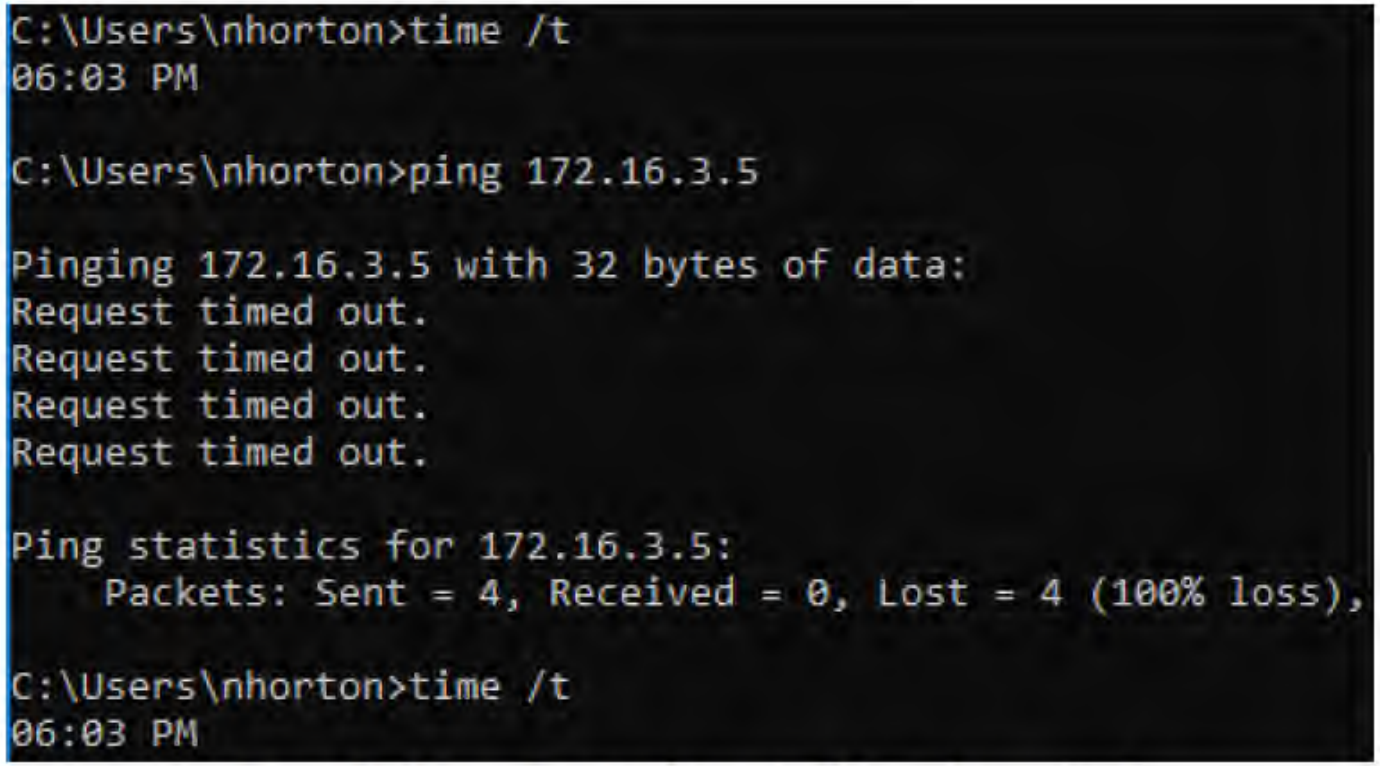
’205 Patent:	TippingPoint:
17… [c] receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;	

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.

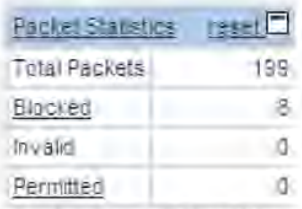
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [c] 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;	 Figure 12: Attempt to ping Computer A from Computer B.

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [c] 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;	 **Figure 13: Attempt to ping Computer B from Computer A.**

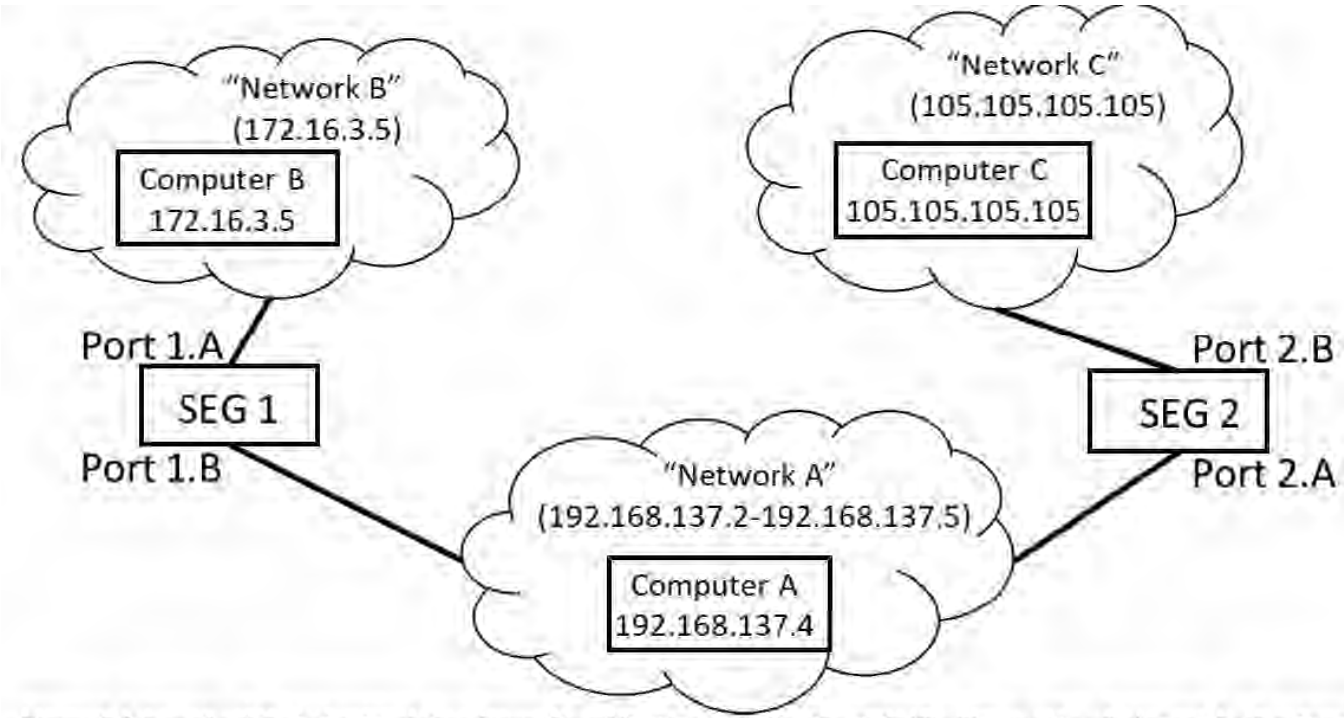
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [c] 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;	 **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.**

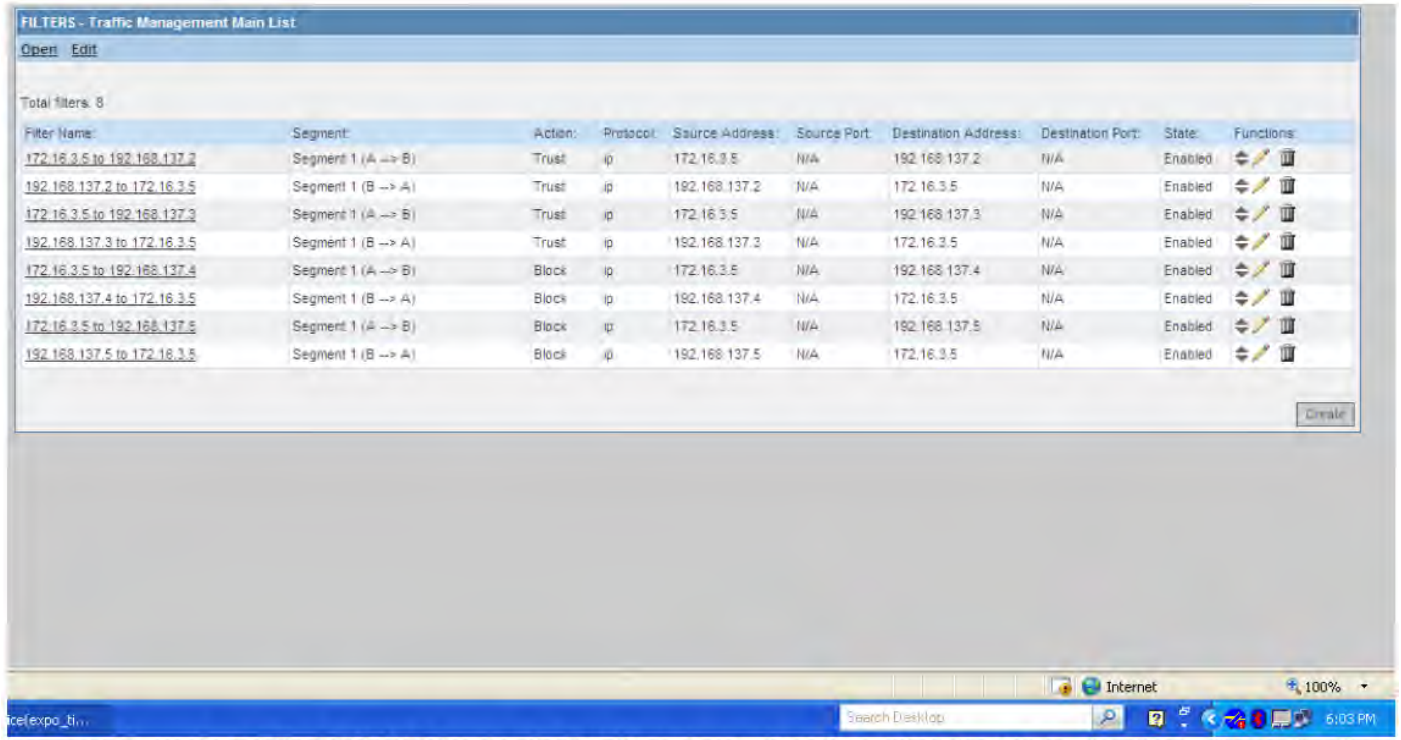
TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[d]** receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	 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.

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[d]** receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	

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)	Block	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)	Block	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

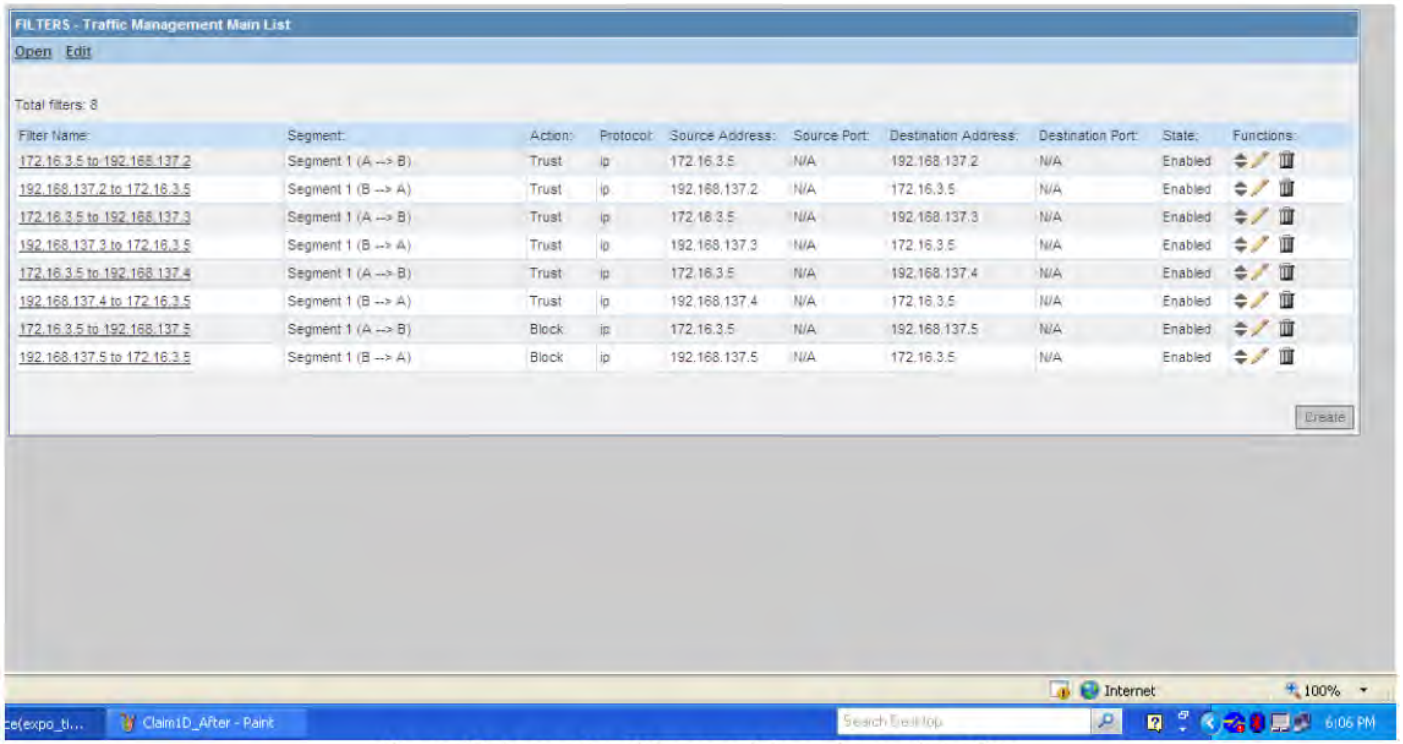
Internet 100% 6:03 PM

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.

TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	

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

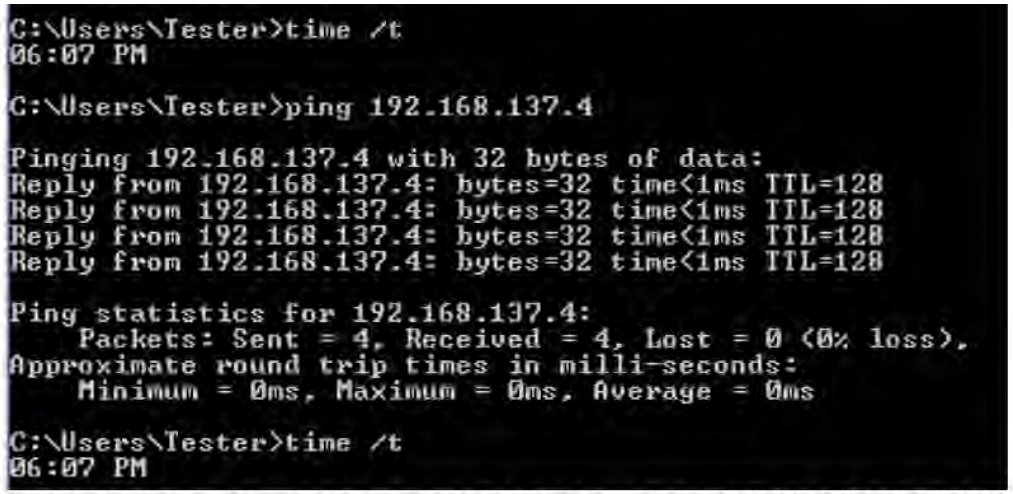
Internet 100%

Claim1D_After - Paint

6:06 PM

Figure 15: Screenshot of the second dynamic security policy.

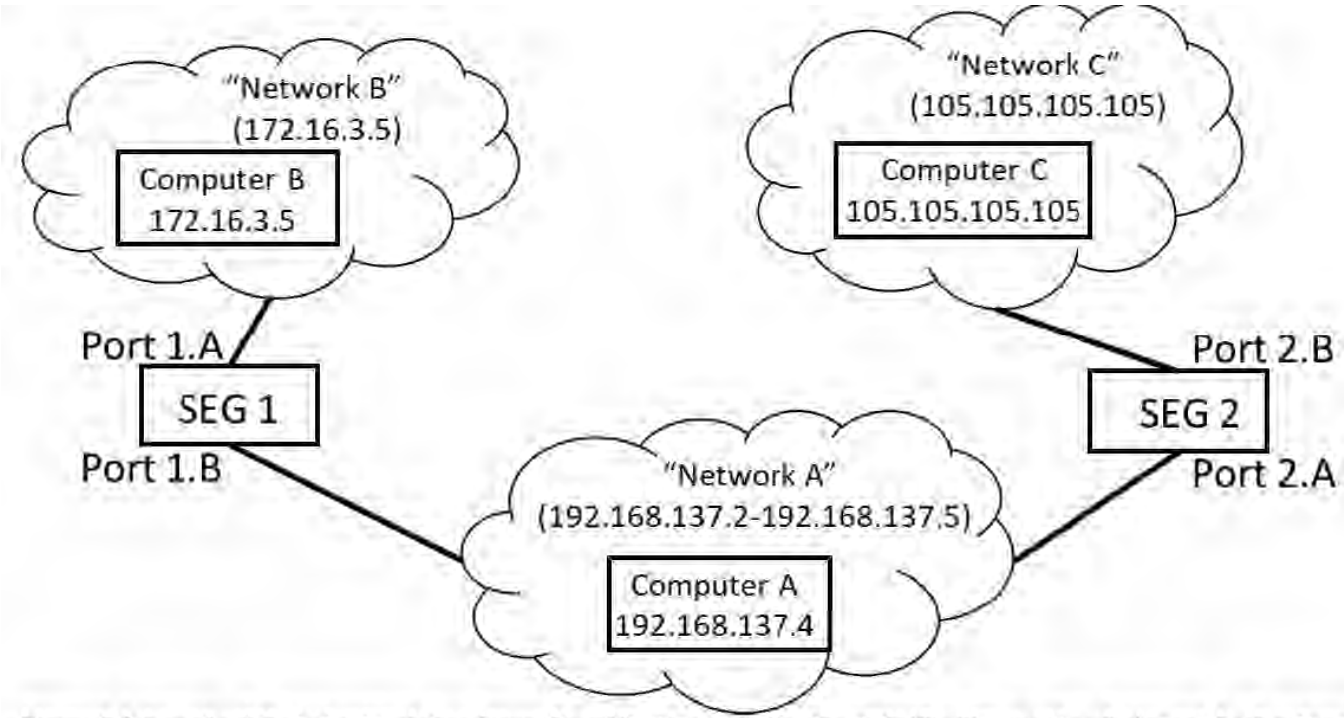
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	 **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.**

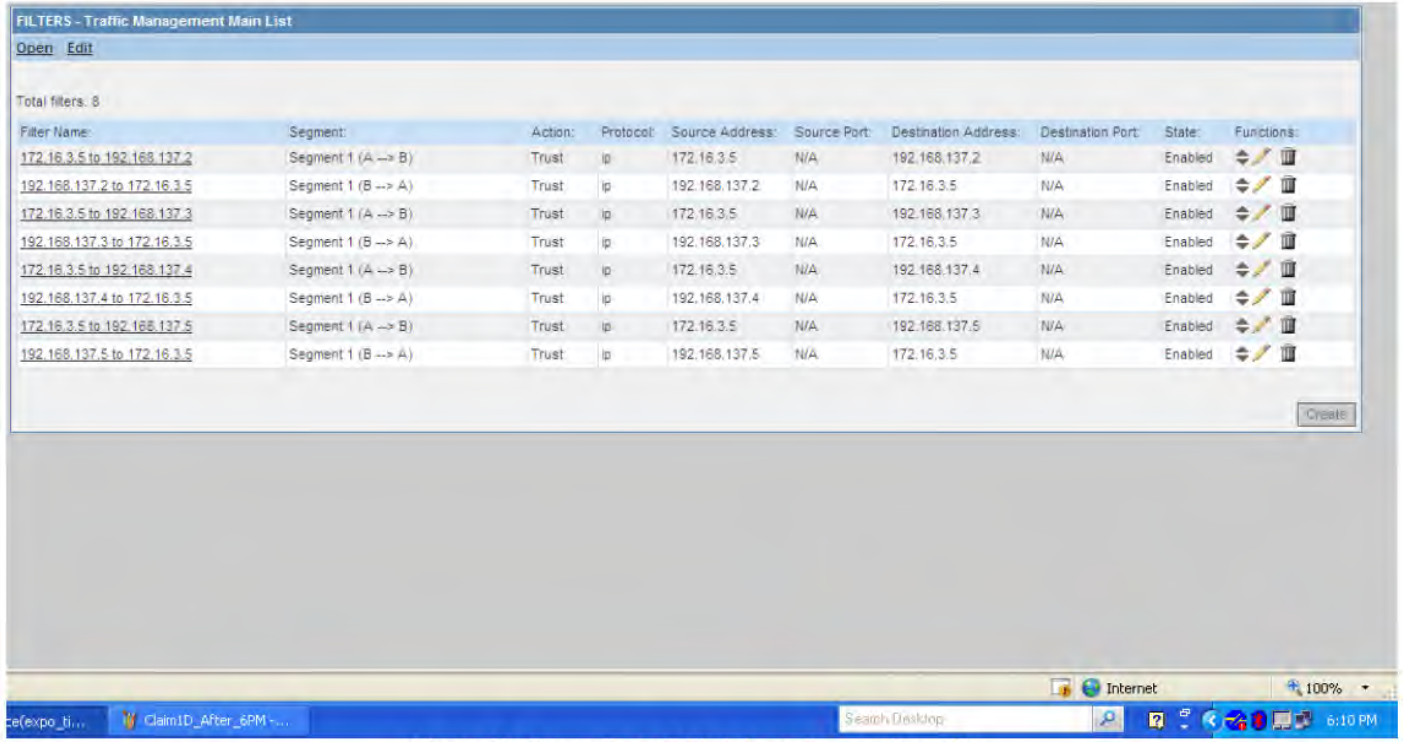
TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [f] 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;	 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.

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [f] 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;	

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%

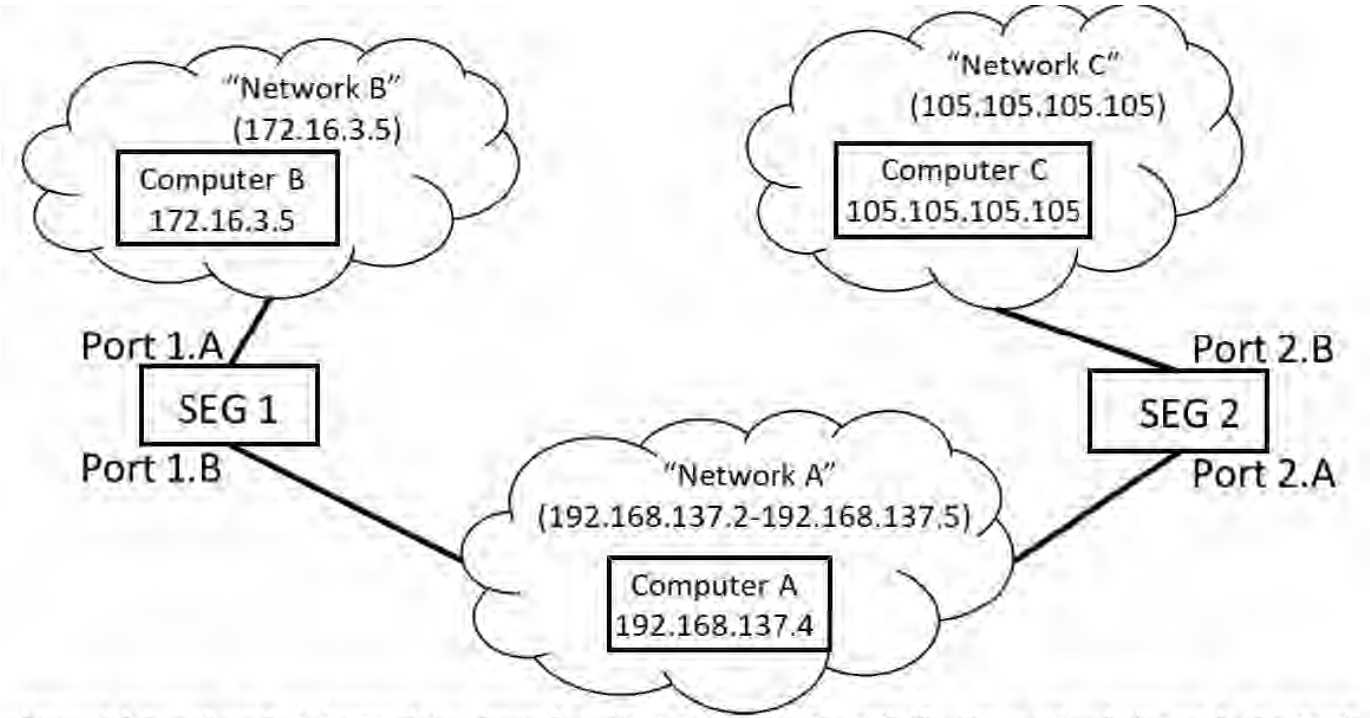
Claim1D_After_6PM -... Search Desktop 6:10 PM

Figure 17: Screenshot of third dynamic security policy.

TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

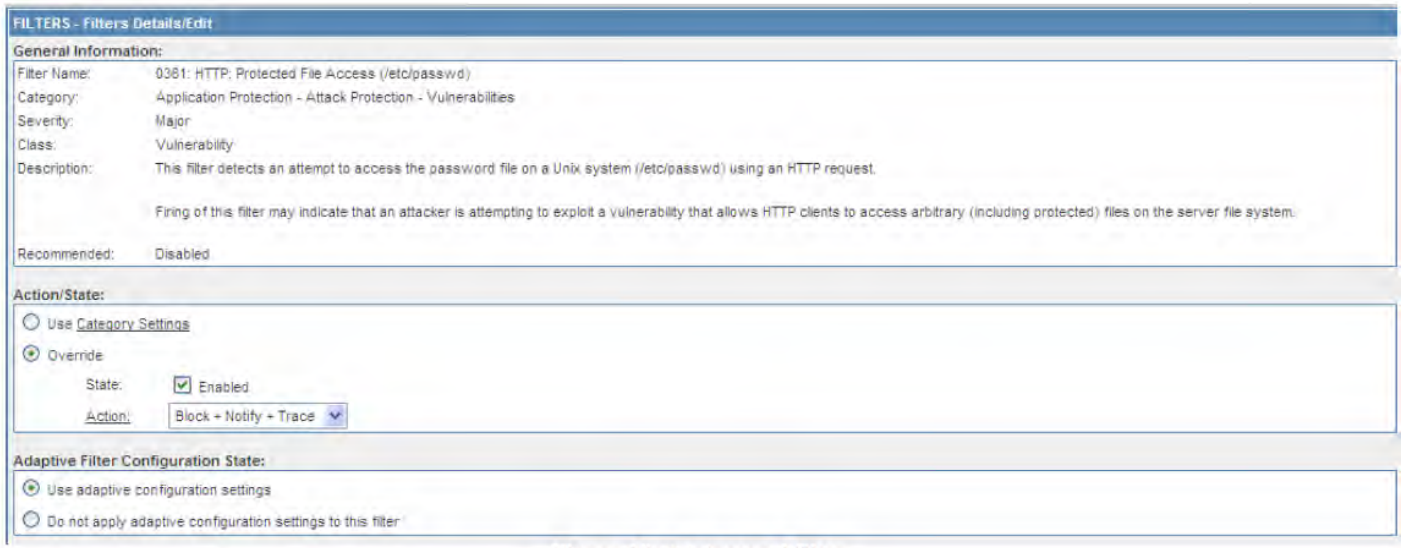
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [g] receive packets associated with a network protected by the packet security gateway; and	 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.

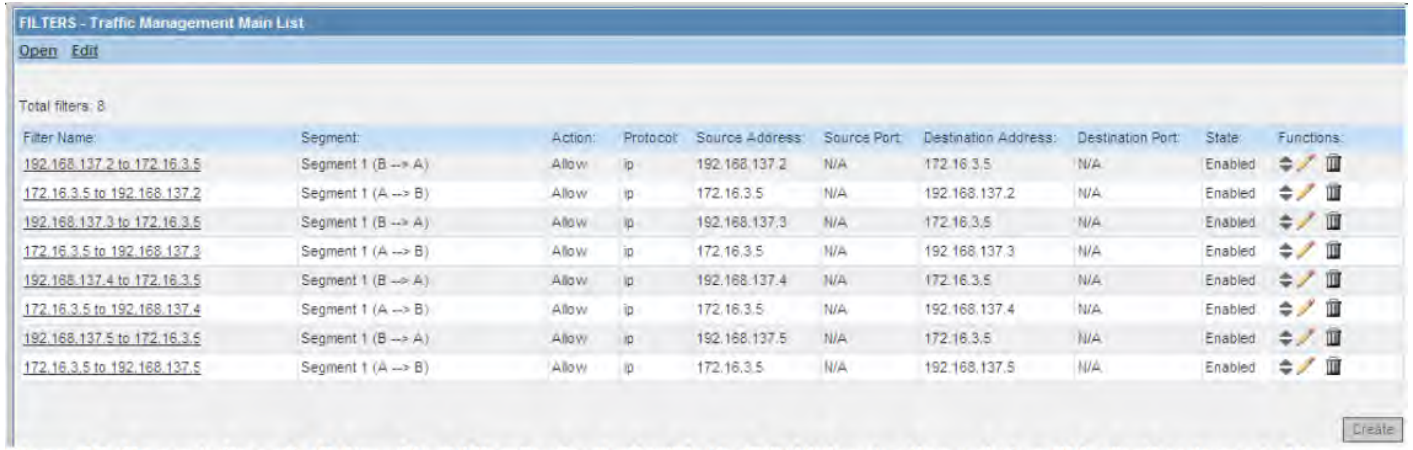
TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[h]** 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.	 **Figure 18: /etc/passwd filter.**

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[h]** 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.	

FILTERS - Traffic Management Main List

Open Edit

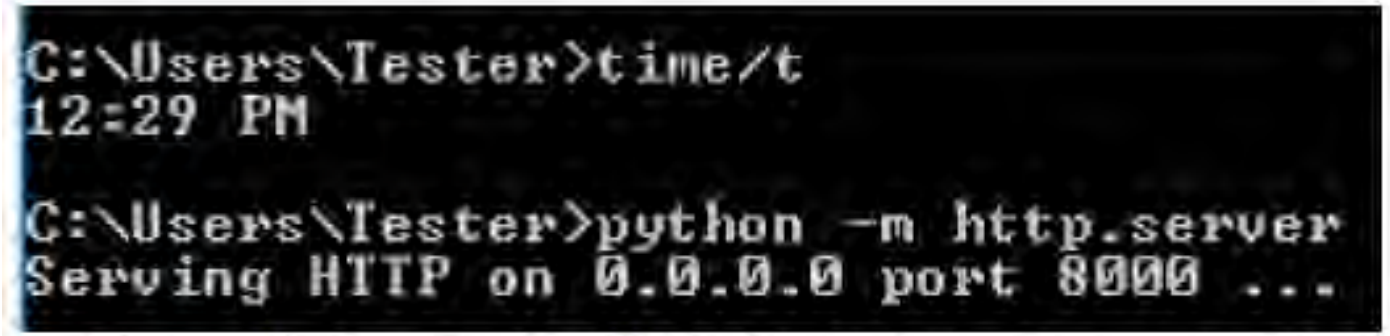
Total filters: 8

Filter Name:	Segment:	Action:	Protocol:	Source Address:	Source Port:	Destination Address:	Destination Port:	State:	Functions:
192.168.137.2 to 172.16.3.5	Segment 1 (B --> A)	Allow	ip	192.168.137.2	N/A	172.16.3.5	N/A	Enabled	
172.16.3.5 to 192.168.137.2	Segment 1 (A --> B)	Allow	ip	172.16.3.5	N/A	192.168.137.2	N/A	Enabled	
192.168.137.3 to 172.16.3.5	Segment 1 (B --> A)	Allow	ip	192.168.137.3	N/A	172.16.3.5	N/A	Enabled	
172.16.3.5 to 192.168.137.3	Segment 1 (A --> B)	Allow	ip	172.16.3.5	N/A	192.168.137.3	N/A	Enabled	
192.168.137.4 to 172.16.3.5	Segment 1 (B --> A)	Allow	ip	192.168.137.4	N/A	172.16.3.5	N/A	Enabled	
172.16.3.5 to 192.168.137.4	Segment 1 (A --> B)	Allow	ip	172.16.3.5	N/A	192.168.137.4	N/A	Enabled	
192.168.137.5 to 172.16.3.5	Segment 1 (B --> A)	Allow	ip	192.168.137.5	N/A	172.16.3.5	N/A	Enabled	
172.16.3.5 to 192.168.137.5	Segment 1 (A --> B)	Allow	ip	172.16.3.5	N/A	192.168.137.5	N/A	Enabled	

Create

Figure 19: Dynamic Security Policy. The “Allow” value in the “Action” field denotes the packets will be further inspected by the IPS.

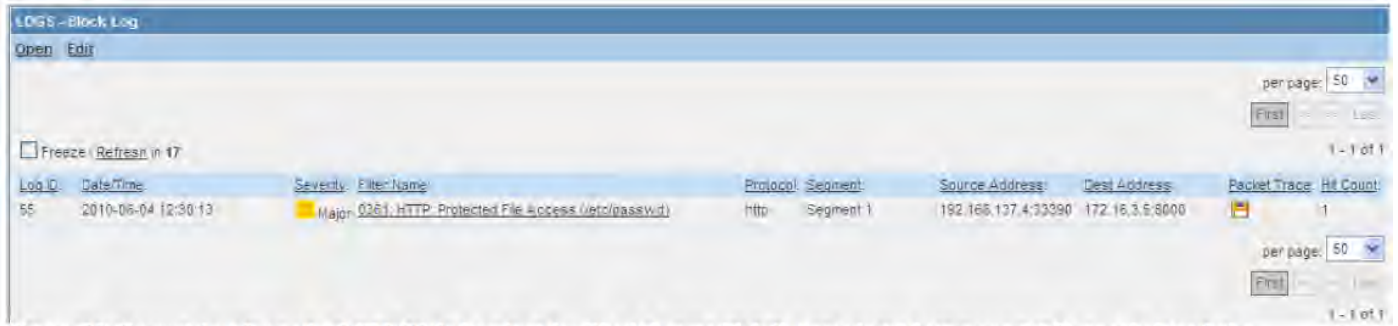
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[h]** 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.	 Figure 20: Hosting the HTTP website on Computer B.

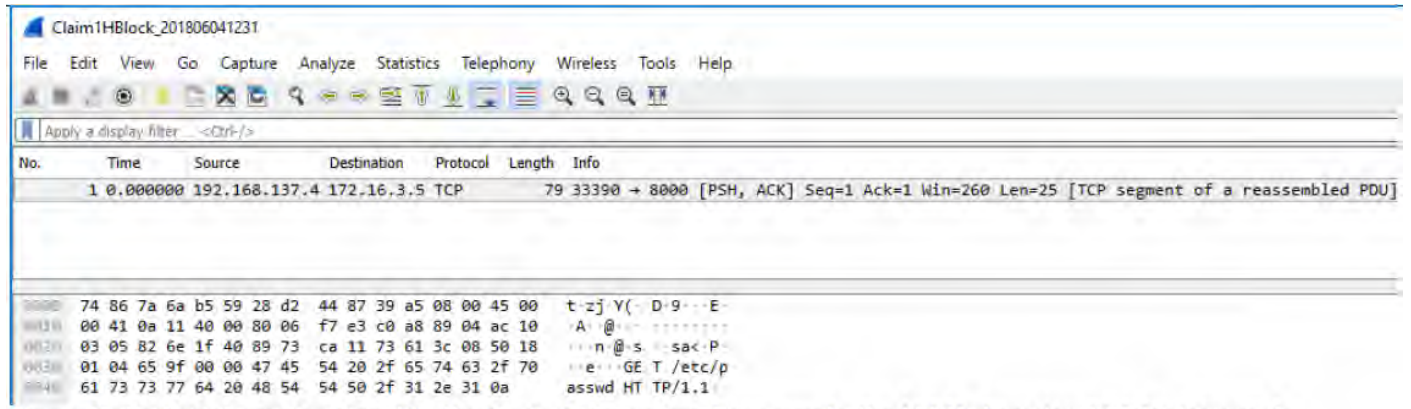
’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… [h] 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.	 **Figure 21: Sending “GET /etc/passwd” request from Computer A (192.168.137.4) to Computer B (172.16.3.5) on port 8000.**

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[h]** 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.	 **Figure 22: Screenshot from the LSM GUI showing the Block Log, which lists packets that were not forwarded to their intended destination.**

’205 Patent Analysis – TippingPoint IPS

’205 Patent:	TippingPoint:
17… **[h]** 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.	 **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.**

TippingPoint IPS Invalidates the ’205 Patent, Claim 17

’205 Patent:	TippingPoint:
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	✓

’205 Patent, Claims 17 and 33 Comparison

17. 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:	33. 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:
receive a plurality of dynamic security policies from the security policy management server,	receive a plurality of dynamic security policies from the security policy management server;
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;	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;
receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;
receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;
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;	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;
receive packets associated with a network protected by the packet security gateway; and	receive packets associated with a network protected by the packet security gateway; 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.	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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 65

TippingPoint IPS Invalidates the ’205 Patent, Claim 33

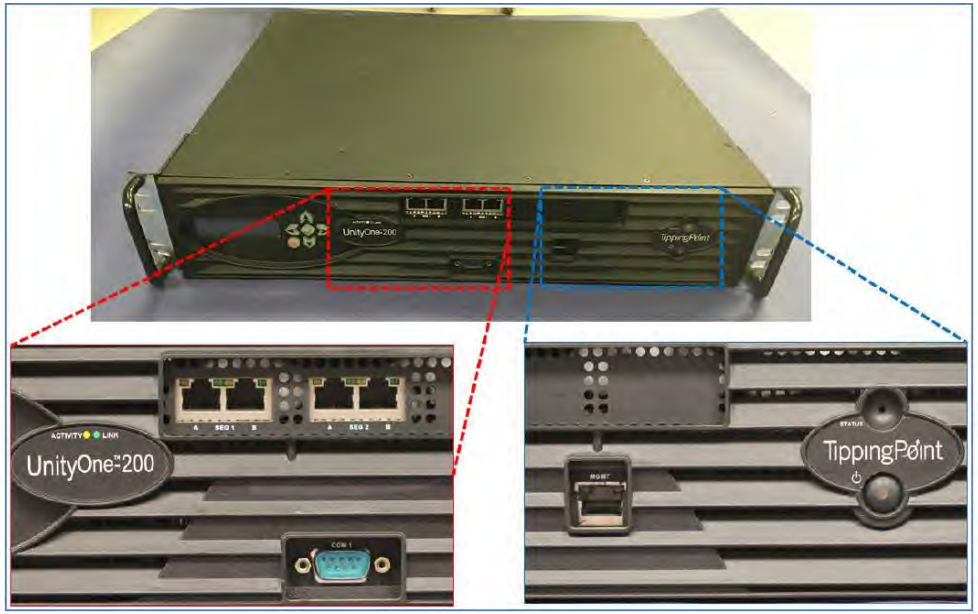
’205 Patent:	TippingPoint:
33. [a] One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	✓

TippingPoint IPS Invalidates the ’722 Patent Claim 1

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

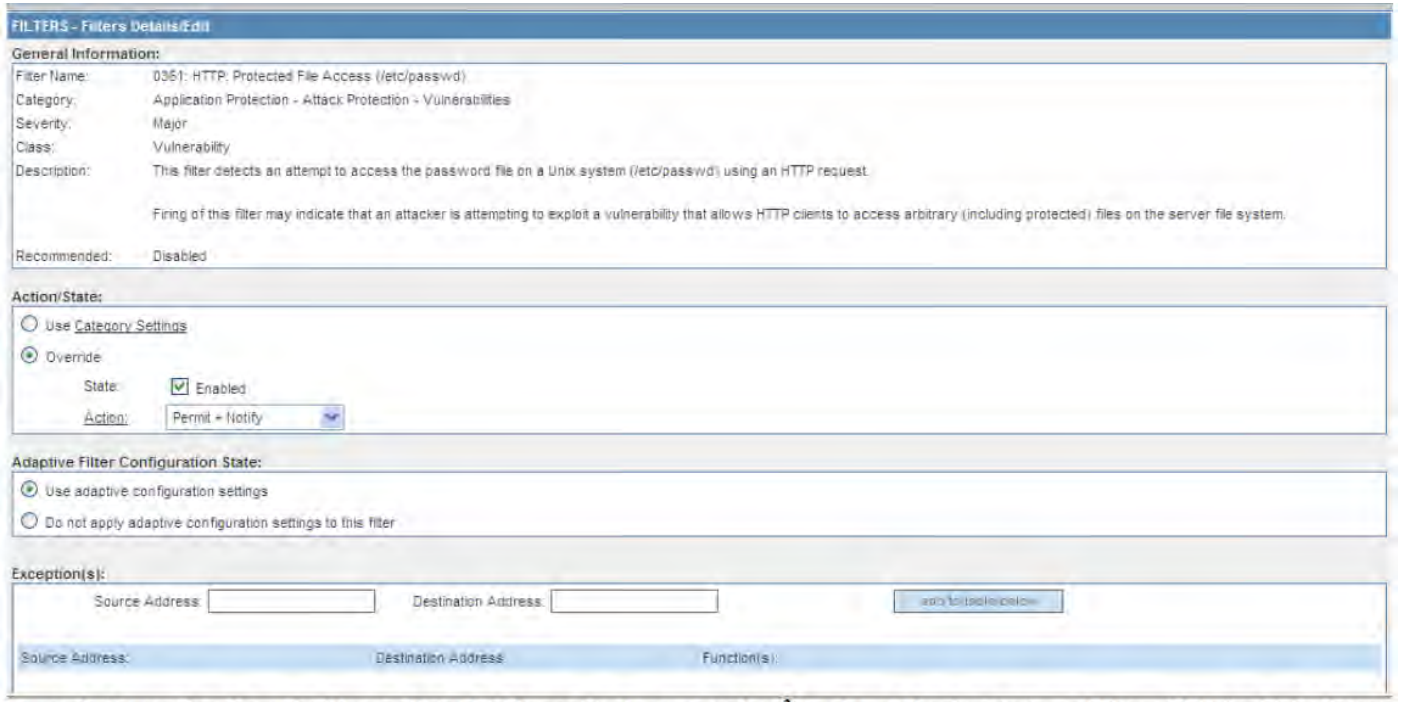
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **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.**

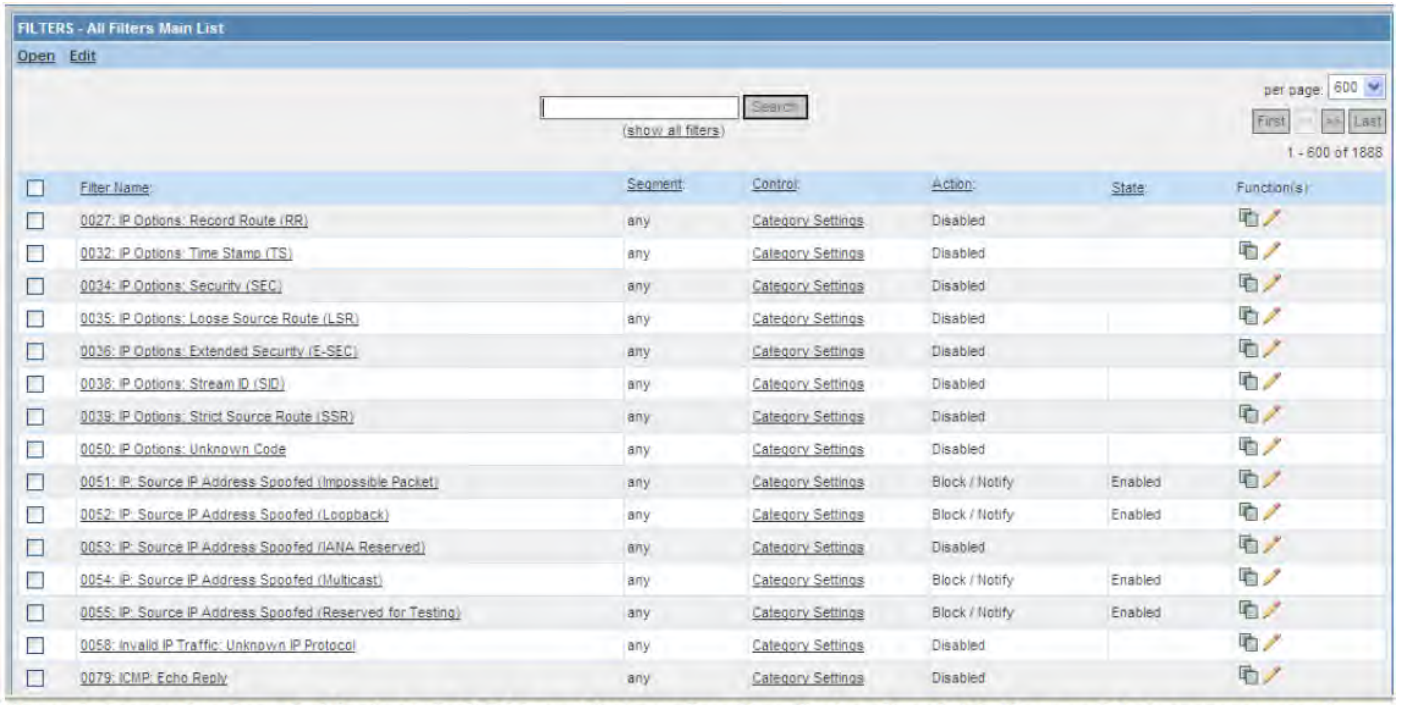
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **Figure 2: TippingPoint IPS hardware showing the part number and serial number of the device.**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **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.”**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1. **[a]** 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;	

FILTERS - All Filters Main List

Open Edit

(show all filters)

per page: 600

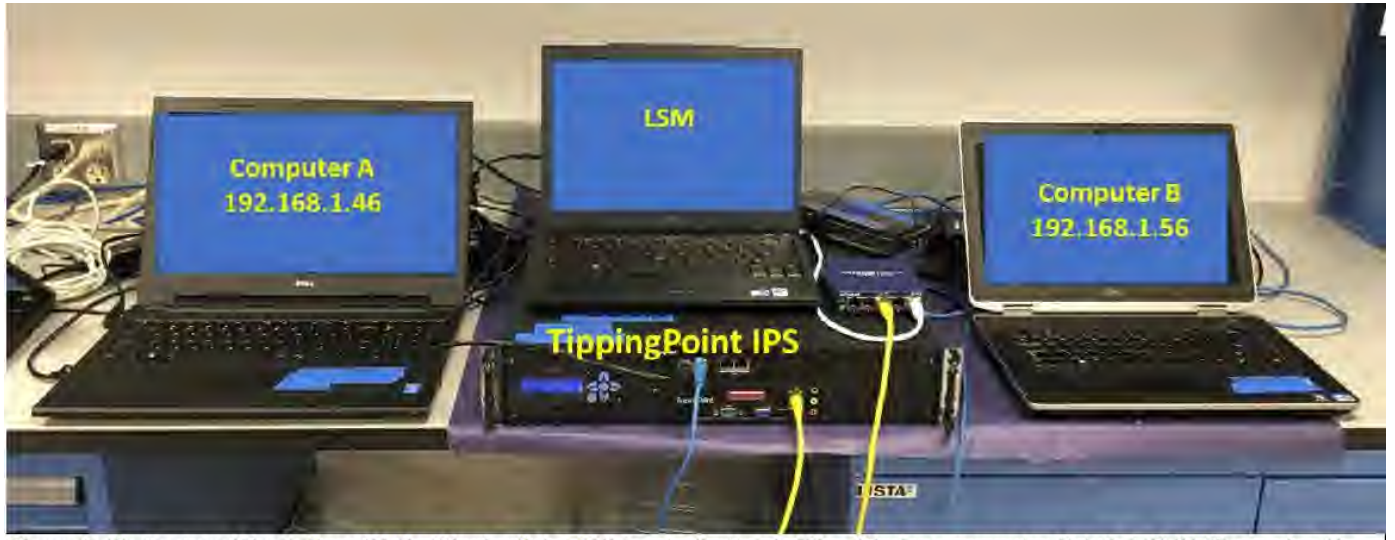
First Last

1 - 600 of 1888

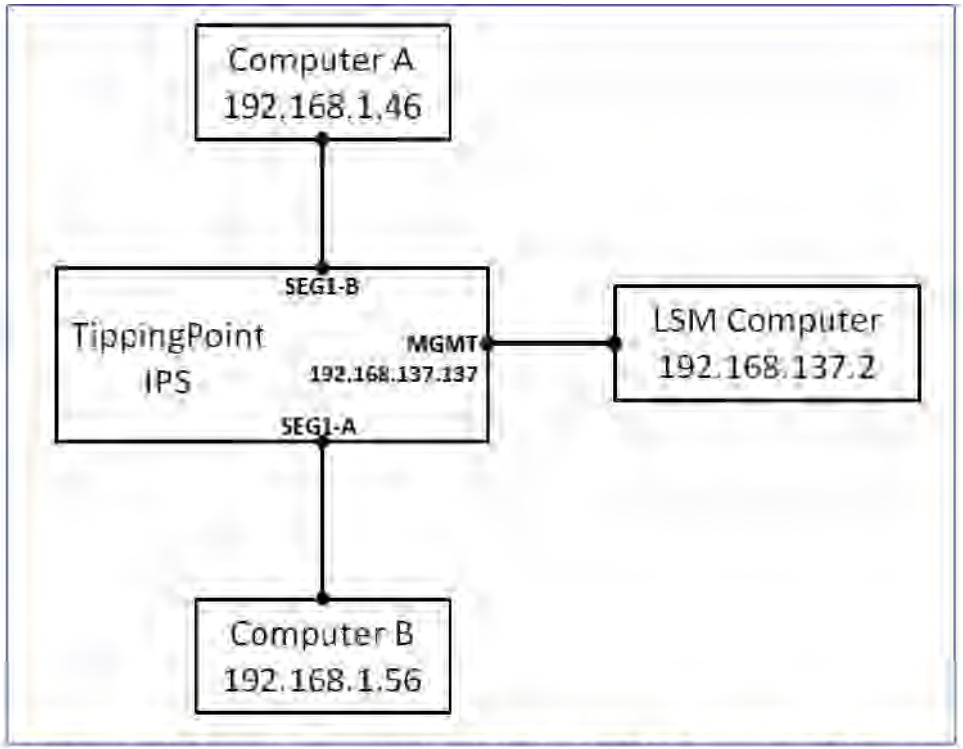
Filter Name	Segment	Control	Action	State	Function(s)
0027: IP Options: Record Route (RR)	any	Category Settings	Disabled		
0032: IP Options: Time Stamp (TS)	any	Category Settings	Disabled		
0034: IP Options: Security (SEC)	any	Category Settings	Disabled		
0035: IP Options: Loose Source Route (LSR)	any	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.

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **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.**

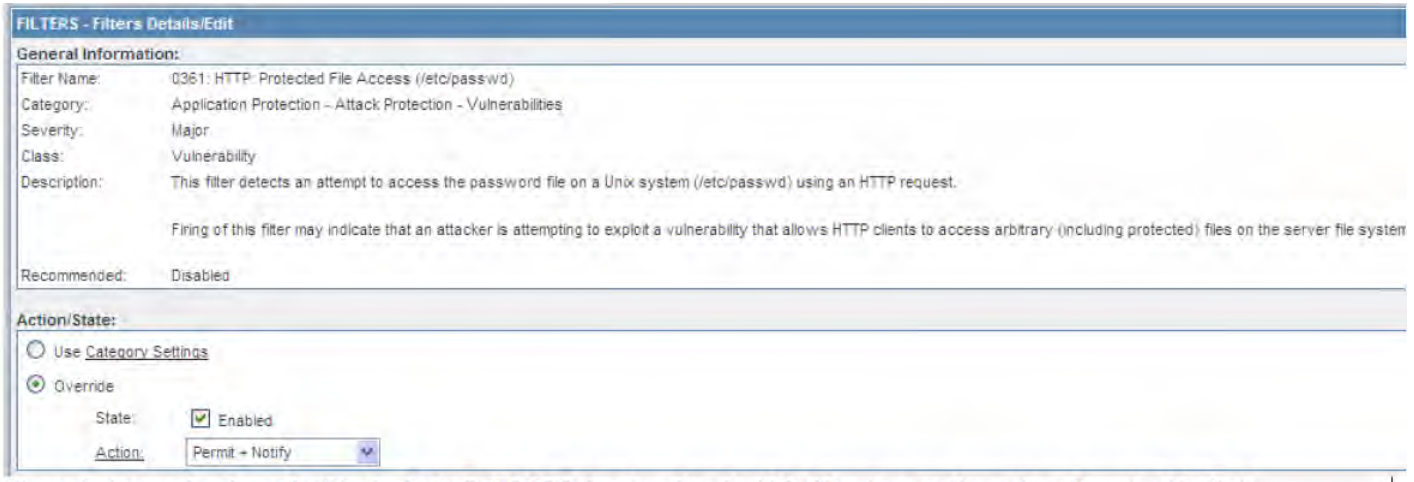
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1. **[a]** 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;	 Figure 6: Network map of test network illustrating connectivity of TippingPoint IPS, Computer A, Computer B, and LSM Computer.

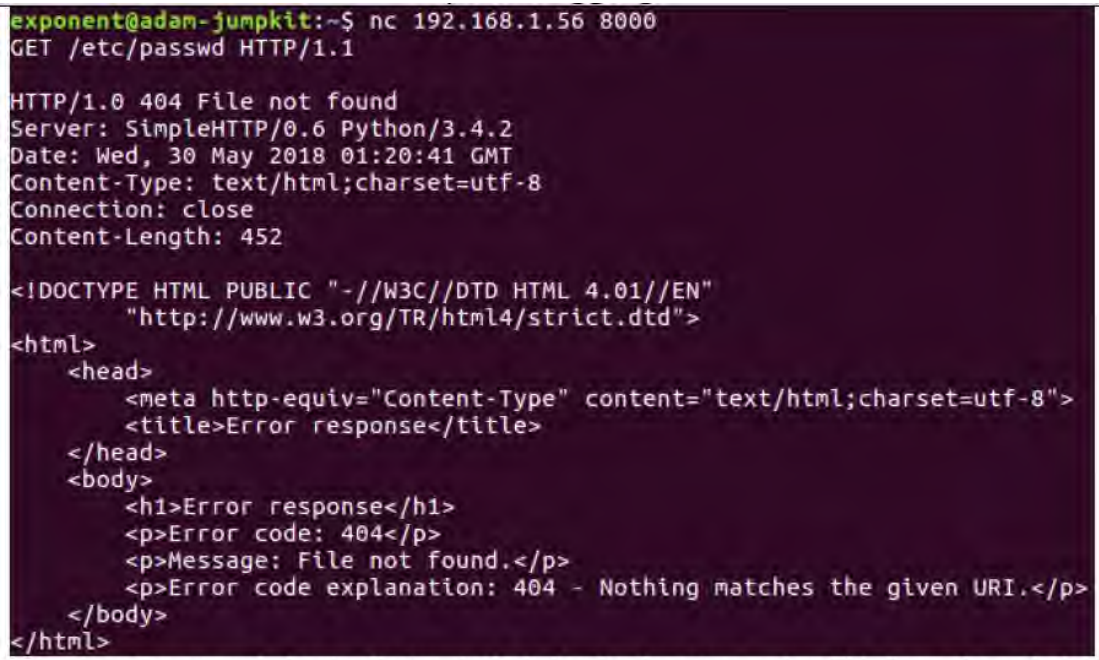
TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	 **Figure 7: Screenshot from the TippingPoint LSM GUI showing that the 0361 filter is set to the action “Permit + Notify.”**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	

```
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

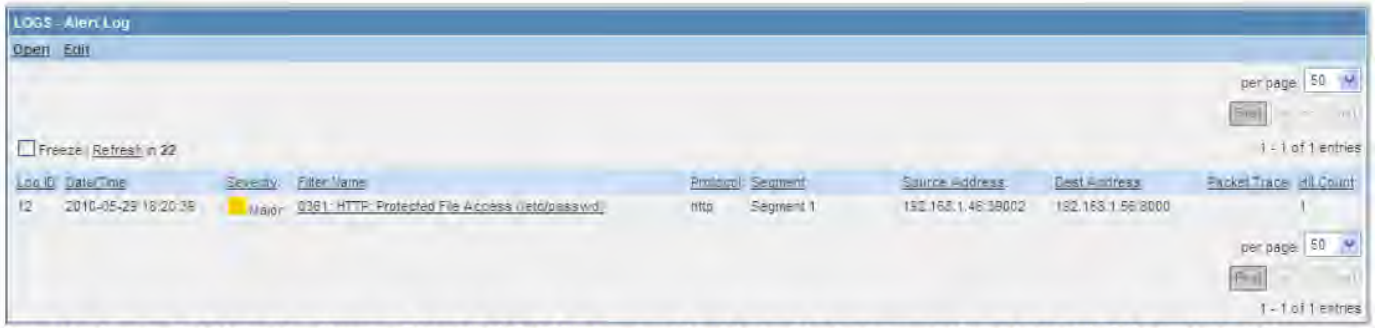
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error 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).

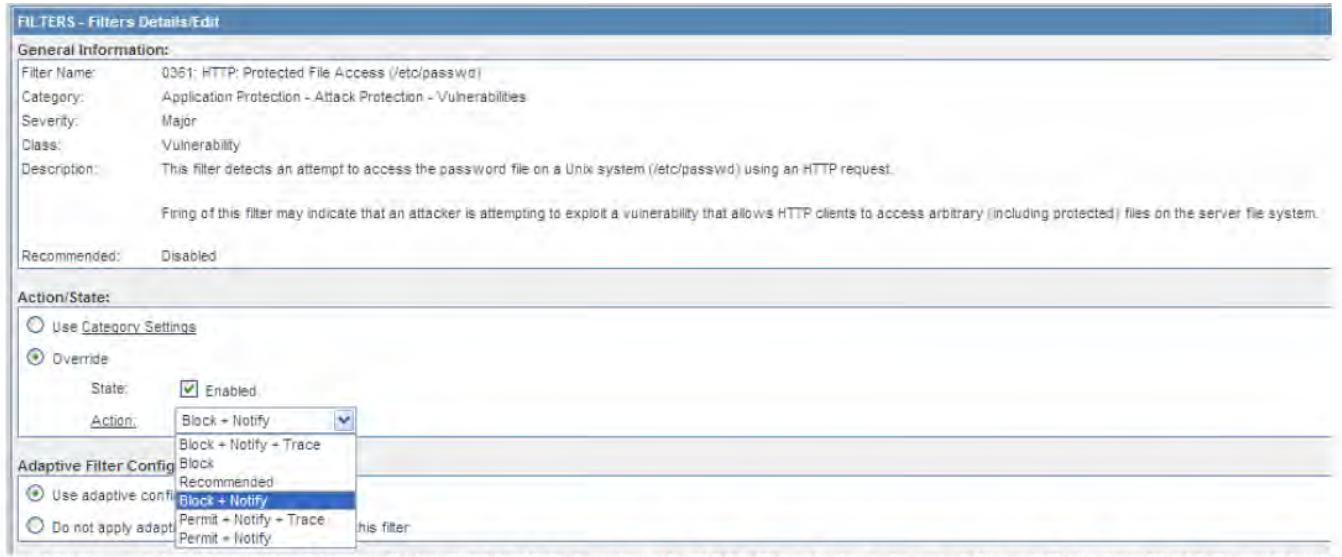
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	 **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.”**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	 **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.**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	 **Figure 11: Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from “Permit + Notify” to “Block + Notify.”**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	 **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).**

’722 Patent Analysis – TippingPoint

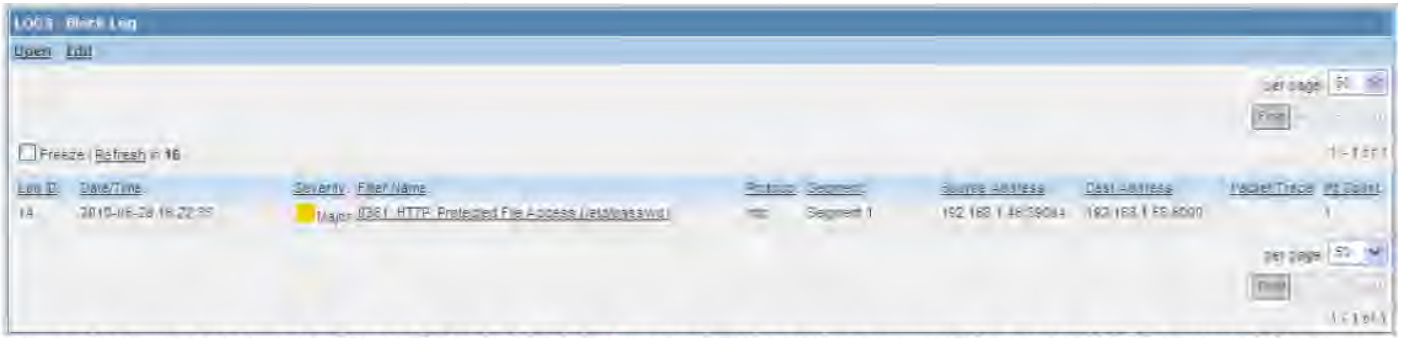
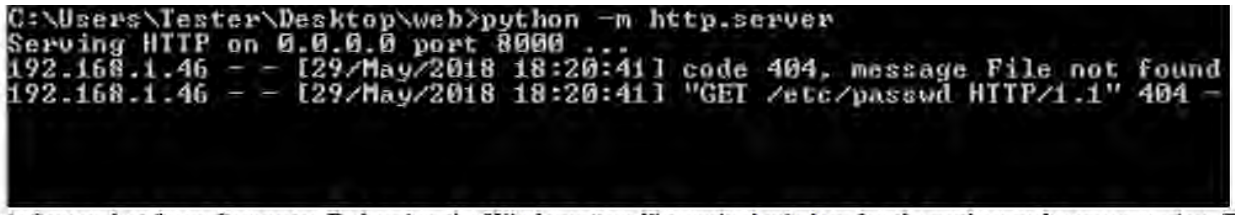
’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	

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).

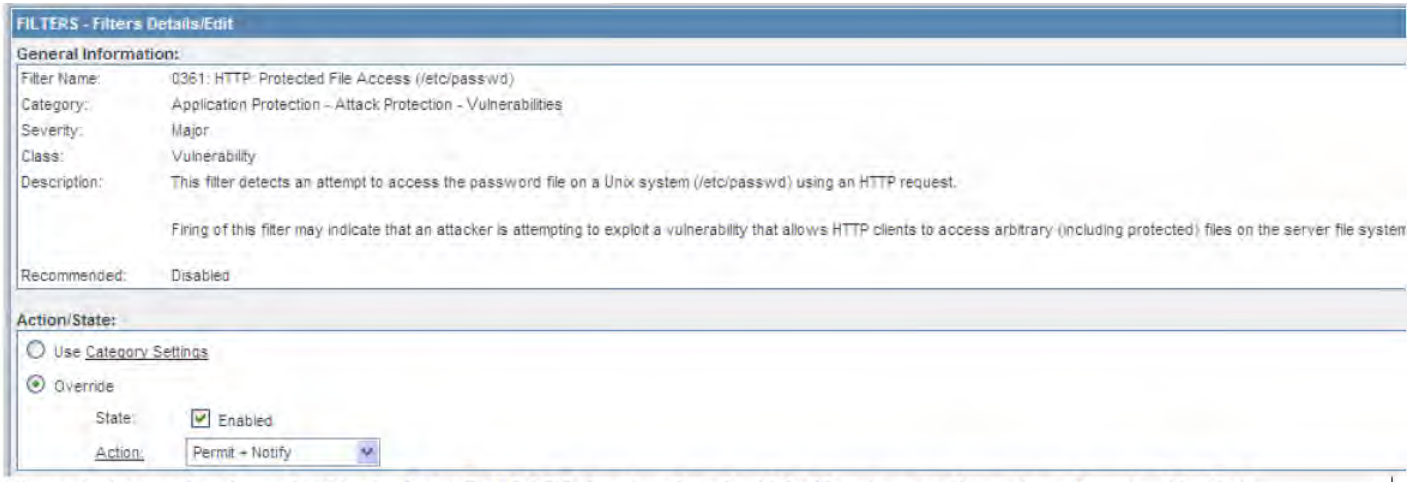
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	 **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.)**

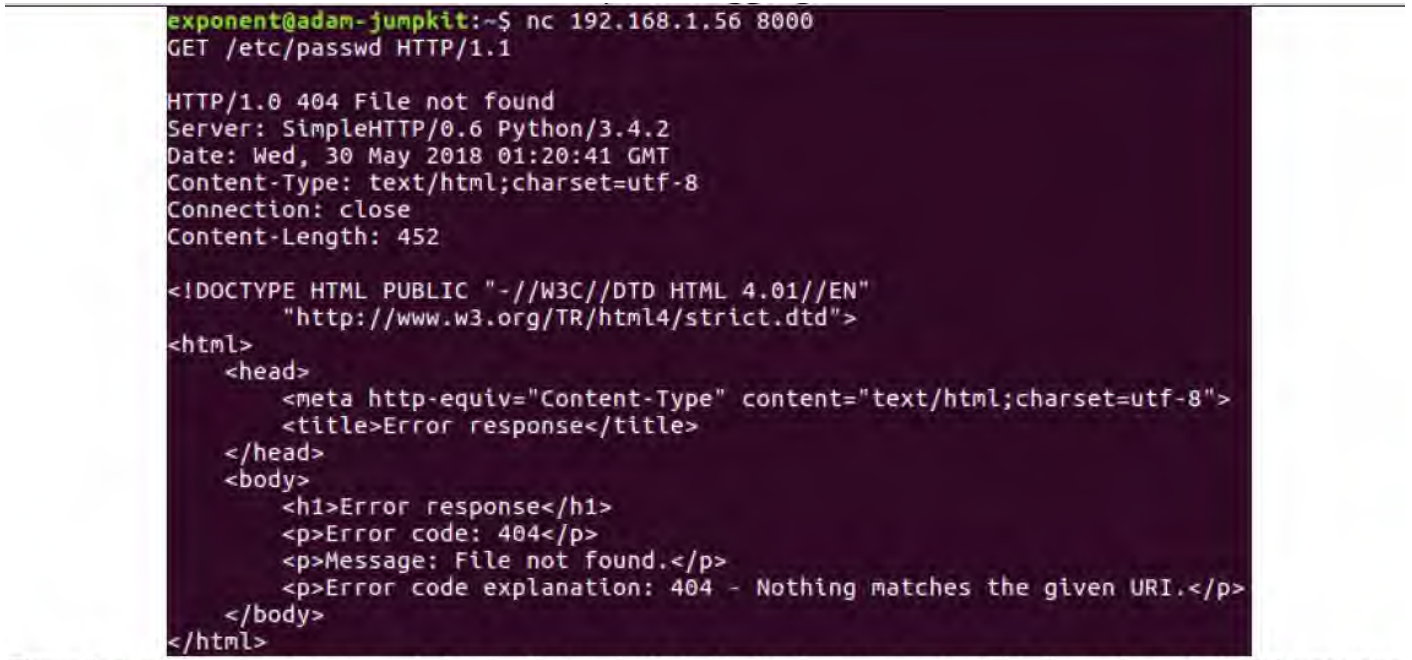
TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[c]** 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;	 **Figure 7: Screenshot from the TippingPoint LSM GUI showing that the 0361 filter is set to the action “Permit + Notify.”**

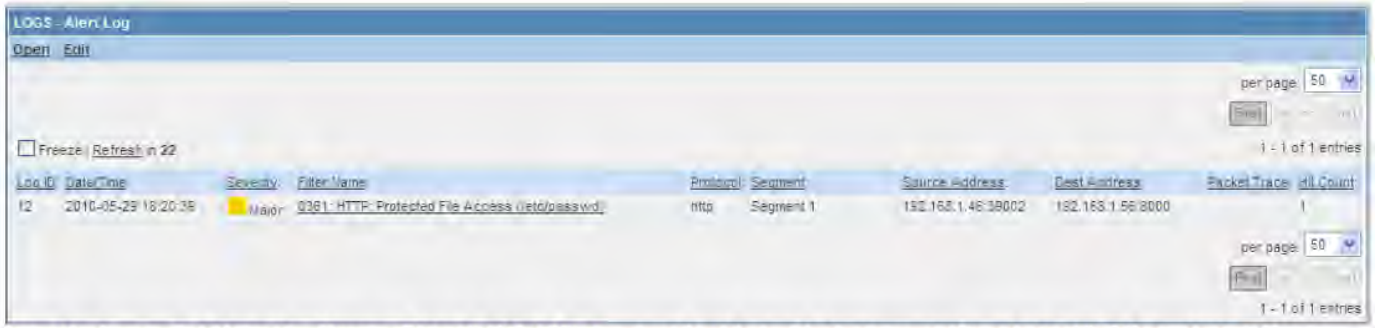
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… [c] 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;	 **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).**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[c]** 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;	 **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.”**

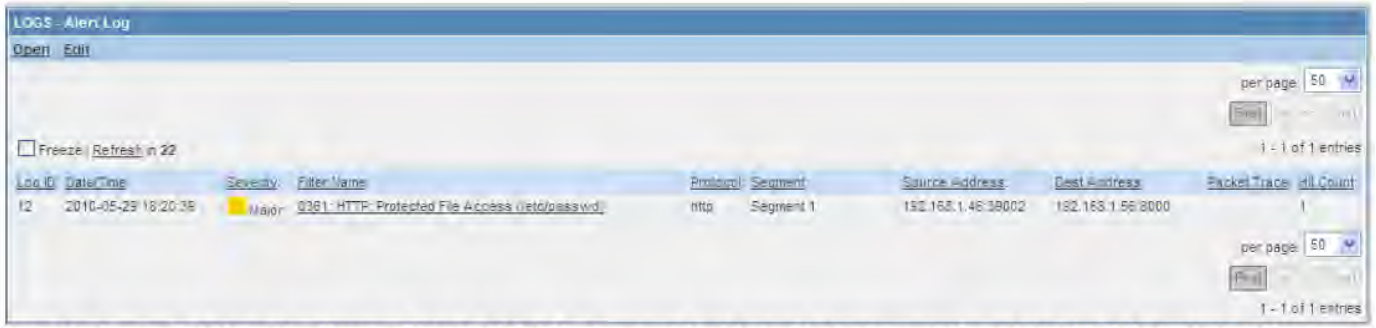
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[c]** 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;	 **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.**

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

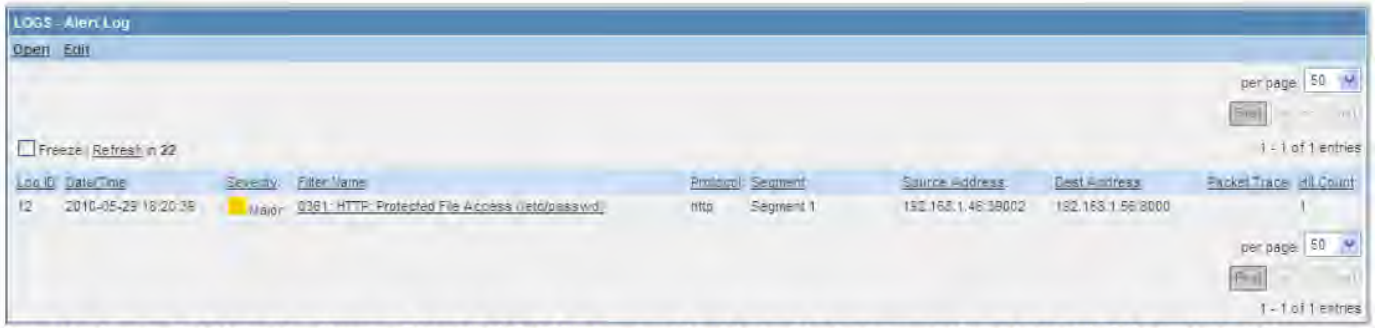
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[d]** 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;	 **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.**

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

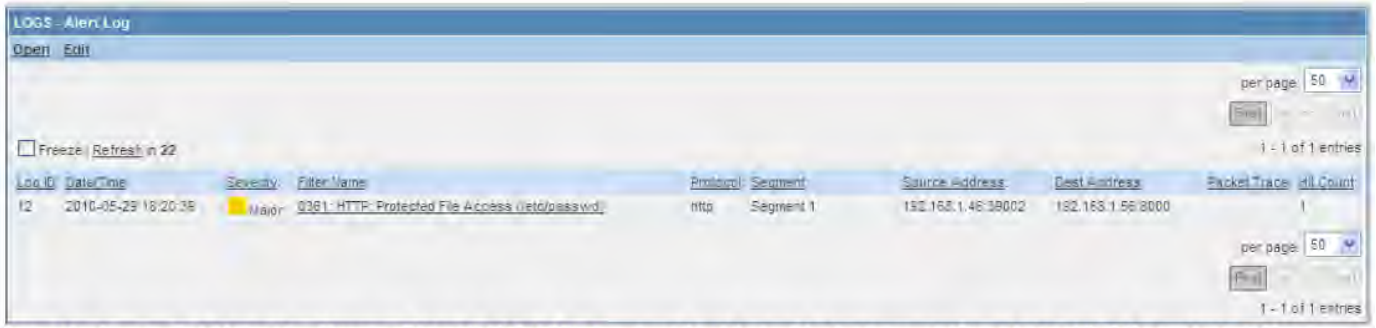
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[e]** 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;	 **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.**

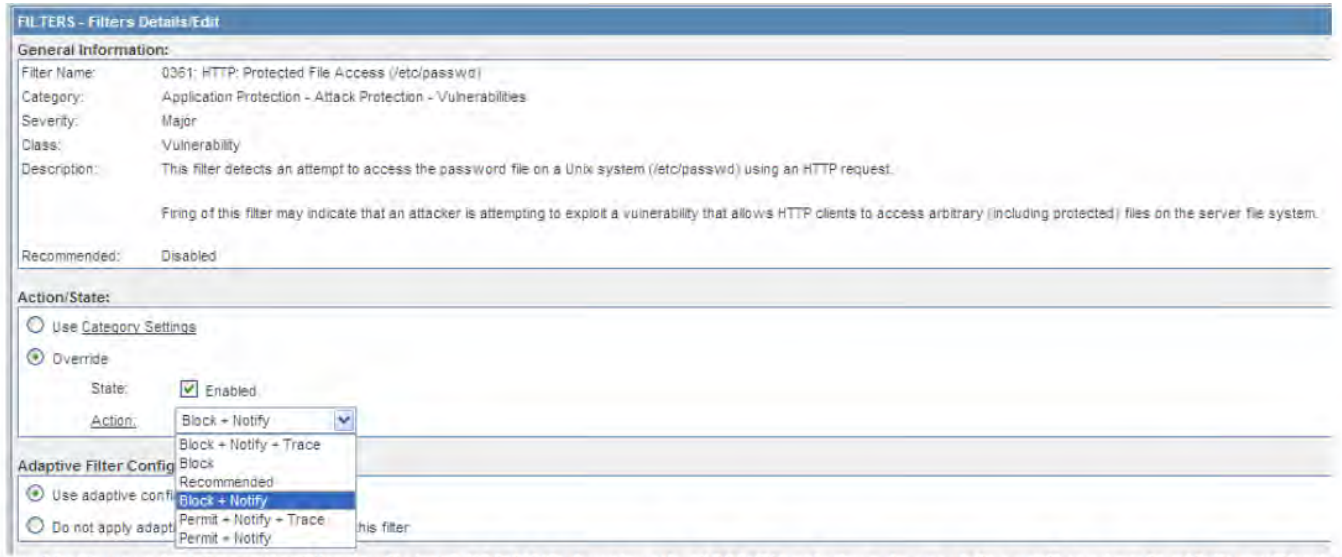
TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[f]** 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	 **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.**

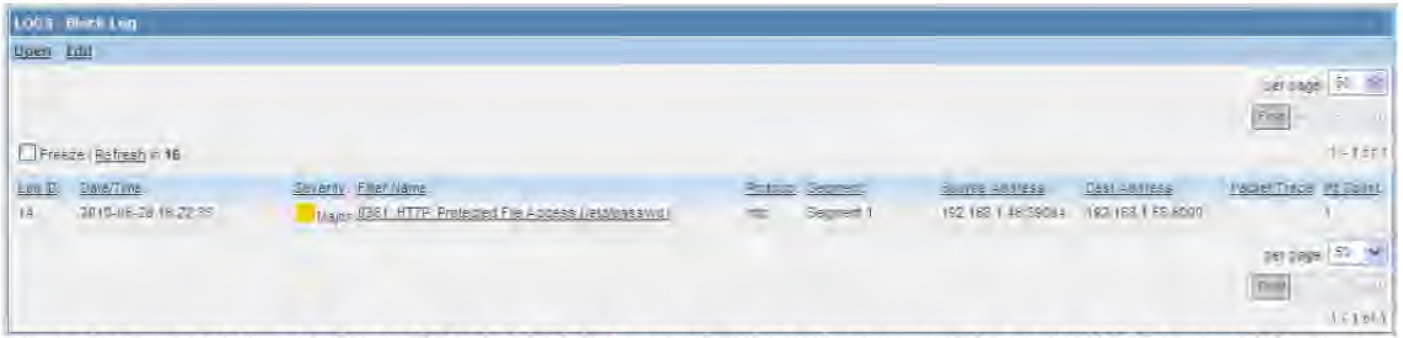
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[f]** 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	 **Figure 11: Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from “Permit + Notify” to “Block + Notify.”**

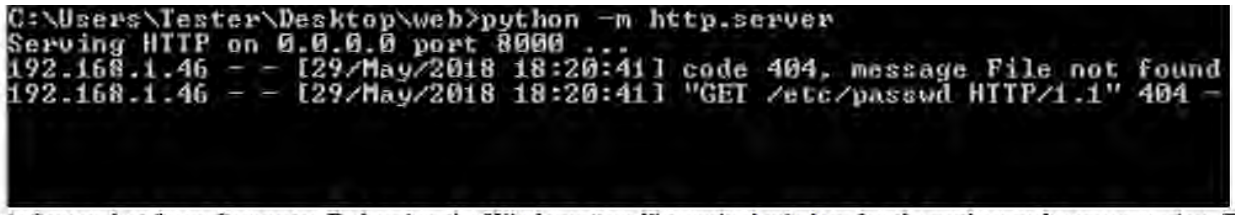
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… [f] 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	 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).

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[f]** 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	 **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).**

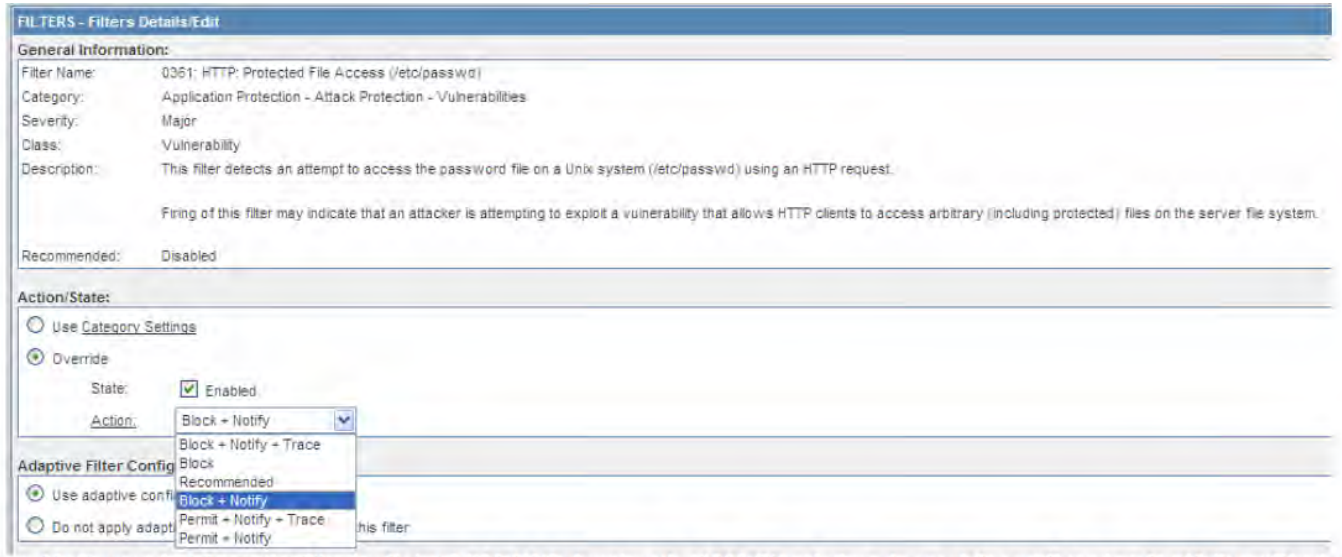
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… [f] 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	 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.)

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – TippingPoint

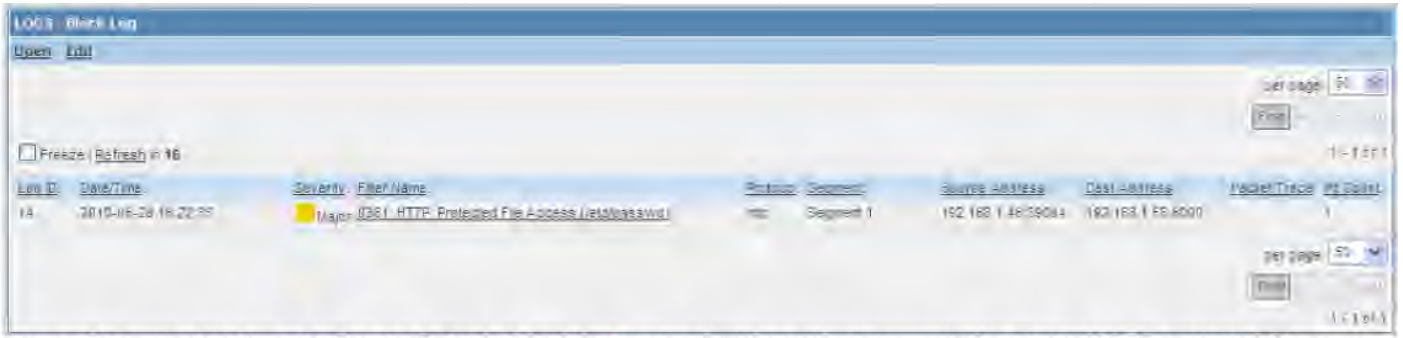
’722 Patent:	TippingPoint:
1… [g] responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and	 **Figure 11: Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from “Permit + Notify” to “Block + Notify.”**

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… [g] 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	 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).

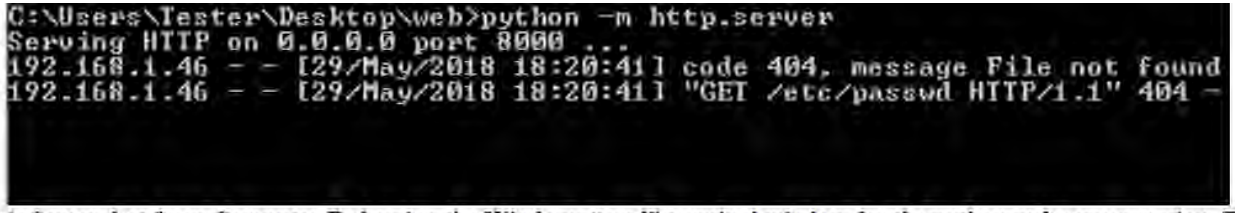
Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 101

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… [g] 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	 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).

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 102

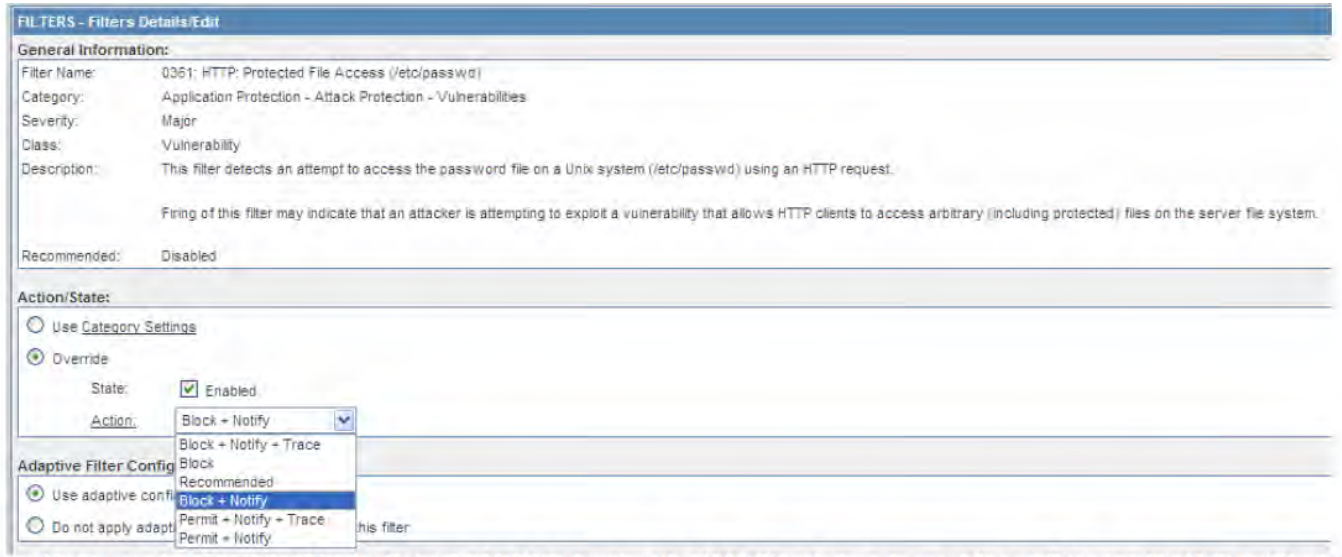
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… [g] 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	 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.)

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

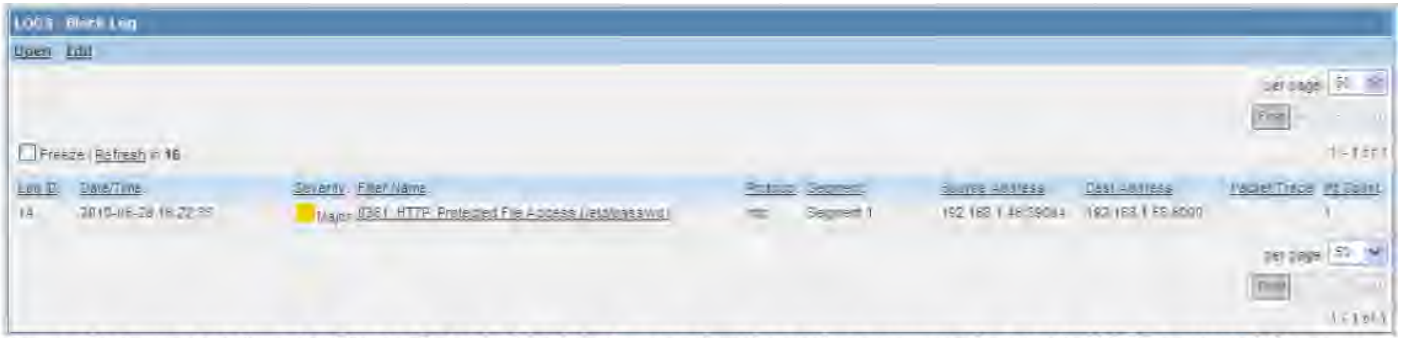
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[h]** 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	 **Figure 11: Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from “Permit + Notify” to “Block + Notify.”**

’722 Patent Analysis – TippingPoint

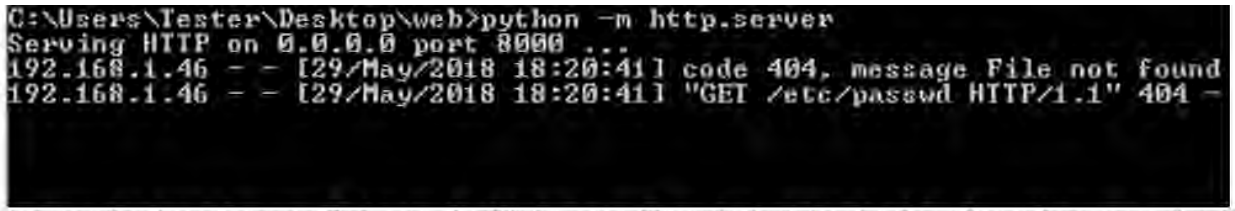
’722 Patent:	TippingPoint:
1… **[h]** responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria: preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet	 Figure 12: Screenshot 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).

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[h]** 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	 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).

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 107

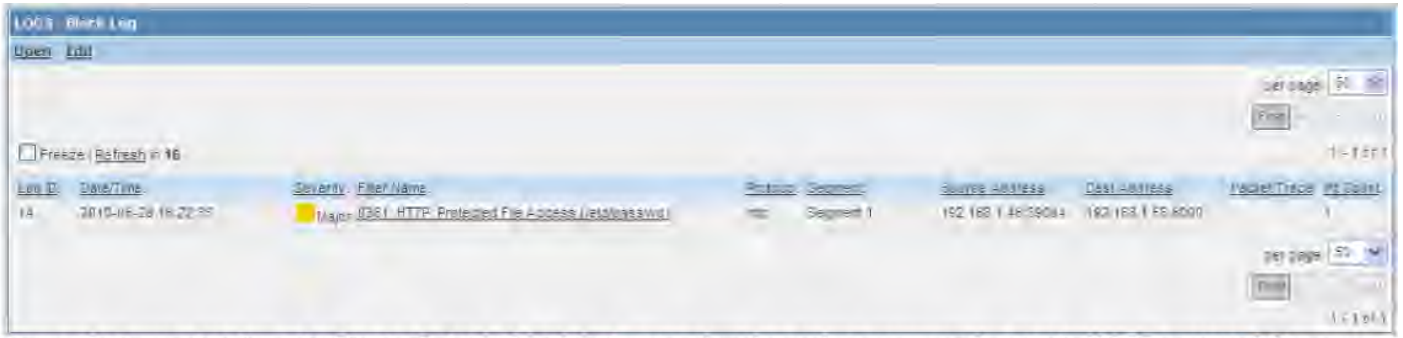
’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… **[h]** 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	 **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.)**

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – TippingPoint

’722 Patent:	TippingPoint:
1… [i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	 **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).**

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	✓
[j] 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.	

’722 Patent Analysis – TippingPoint

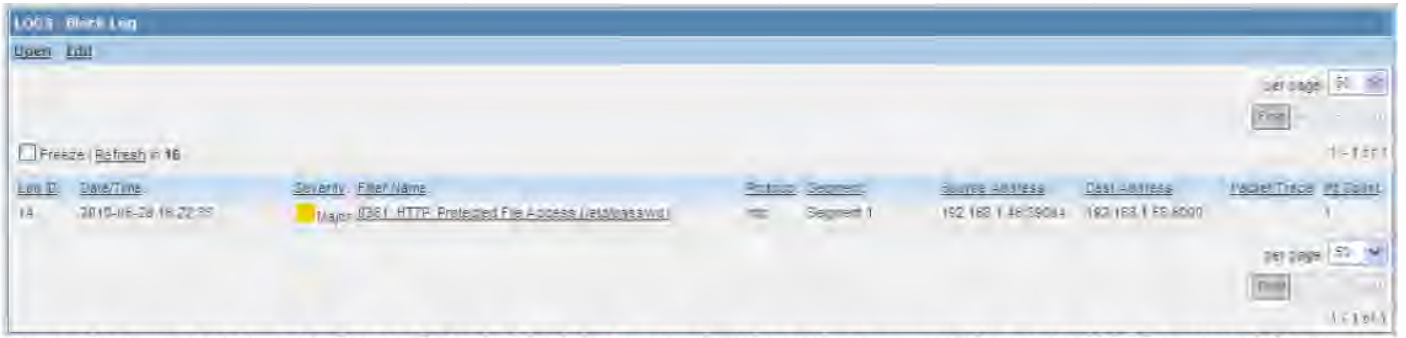
’722 Patent:	TippingPoint:
1… [j] causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.	

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).

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 112

TippingPoint IPS Invalidates the ’722 Patent, Claim 1

’722 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	✓
[j] 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.	✓

TippingPoint IPS Invalidates the ’213 Patent Claim 1

TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. [a] 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;	
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

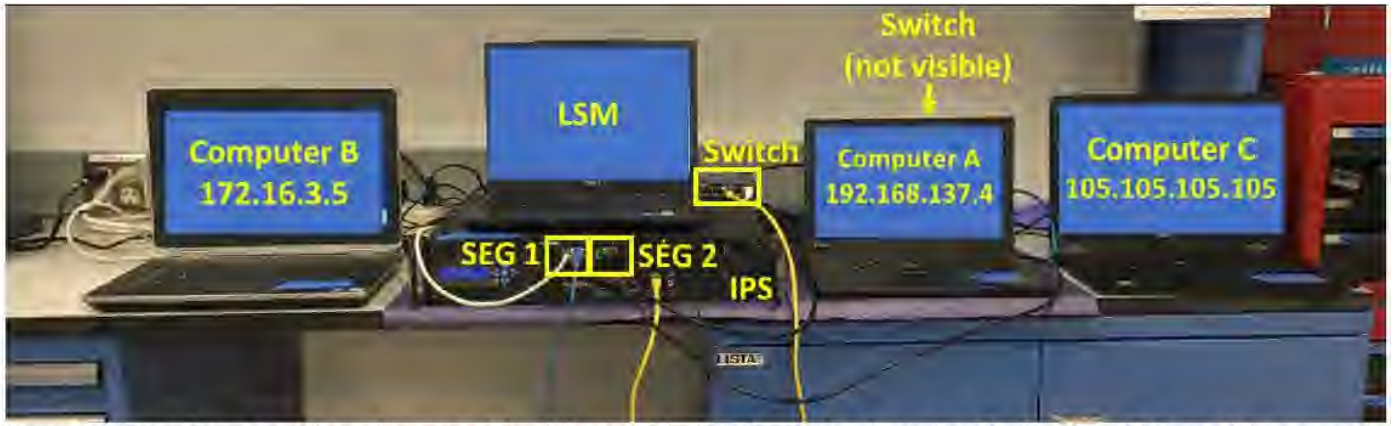
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **Figure 1: TippingPoint IPS hardware showing the part number and serial number of the device.**

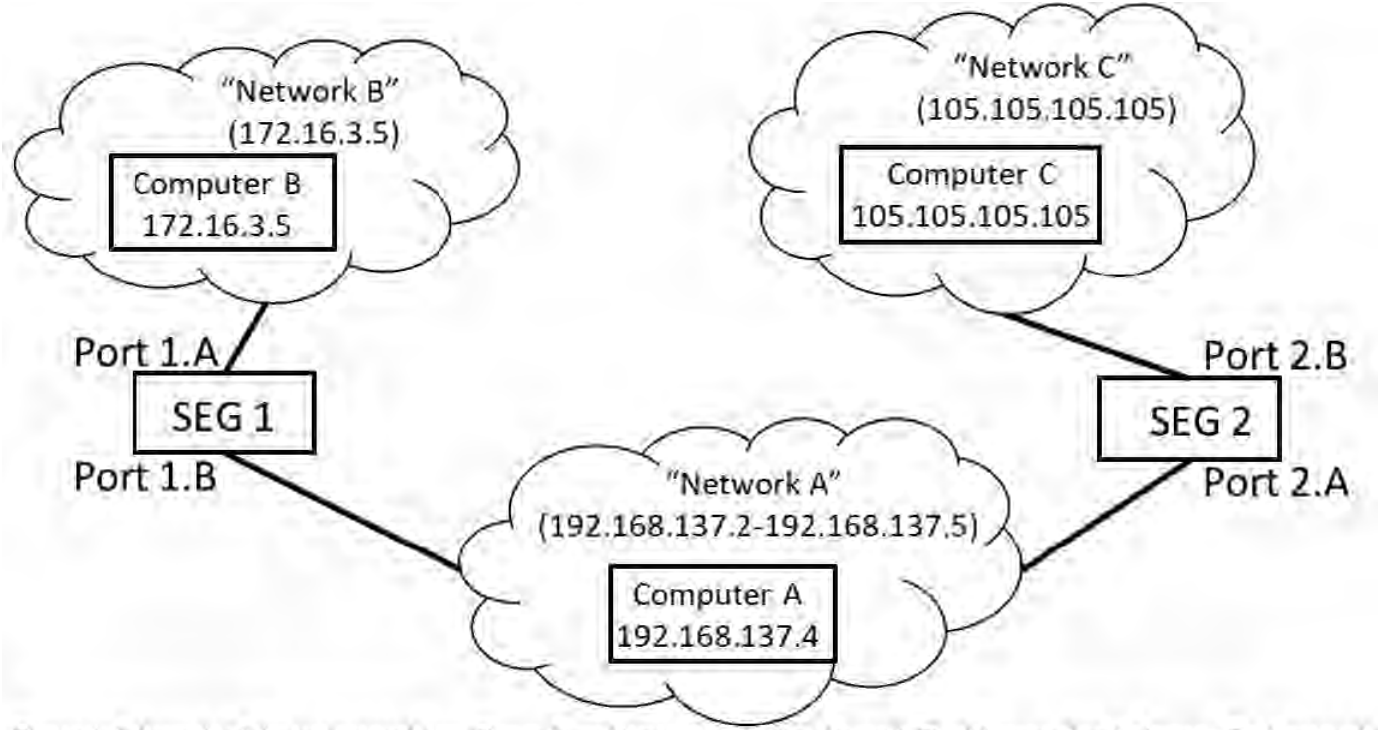
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **Figure 2: Annotated photographs of the TippingPoint IPS showing two packet security gateway interfaces (lower left) and one management interface (lower right).**

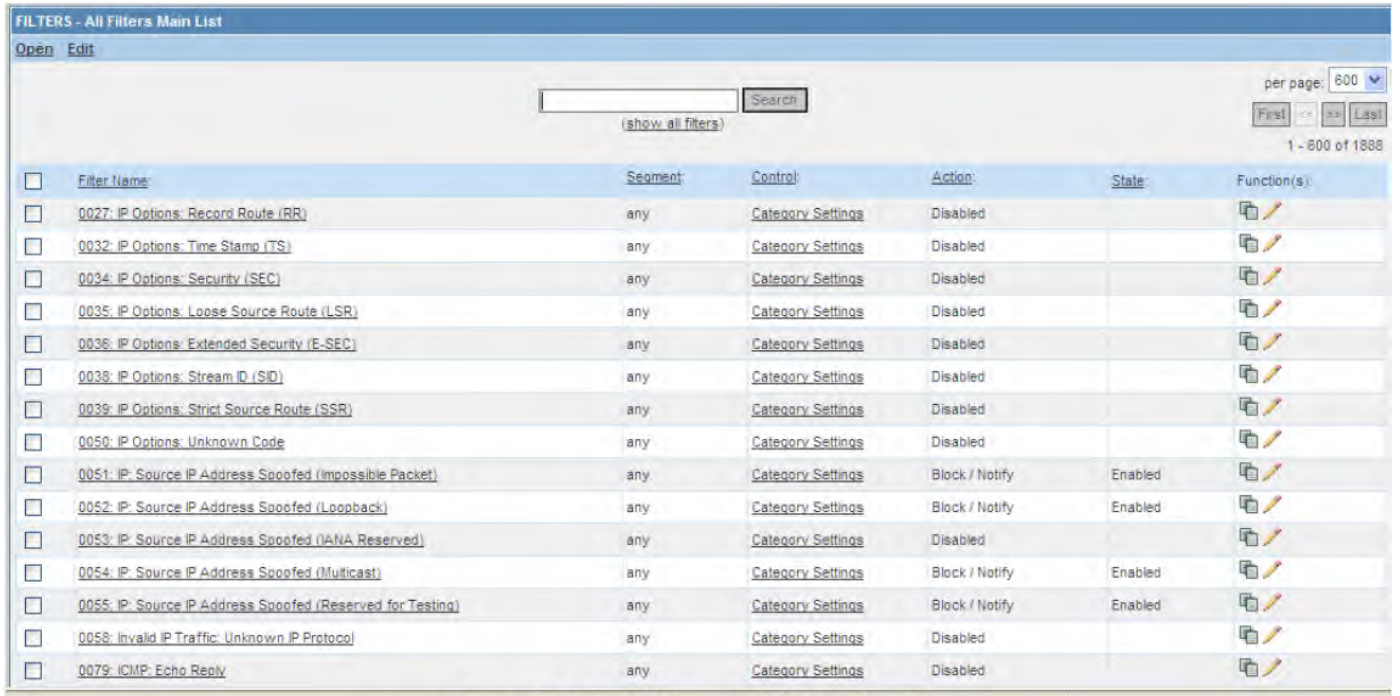
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **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.**

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1. **[a]** 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;	 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.

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1. **[a]** 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;	

FILTERS - All Filters Main List

Open Edit

Search

(show all filters)

per page: 600

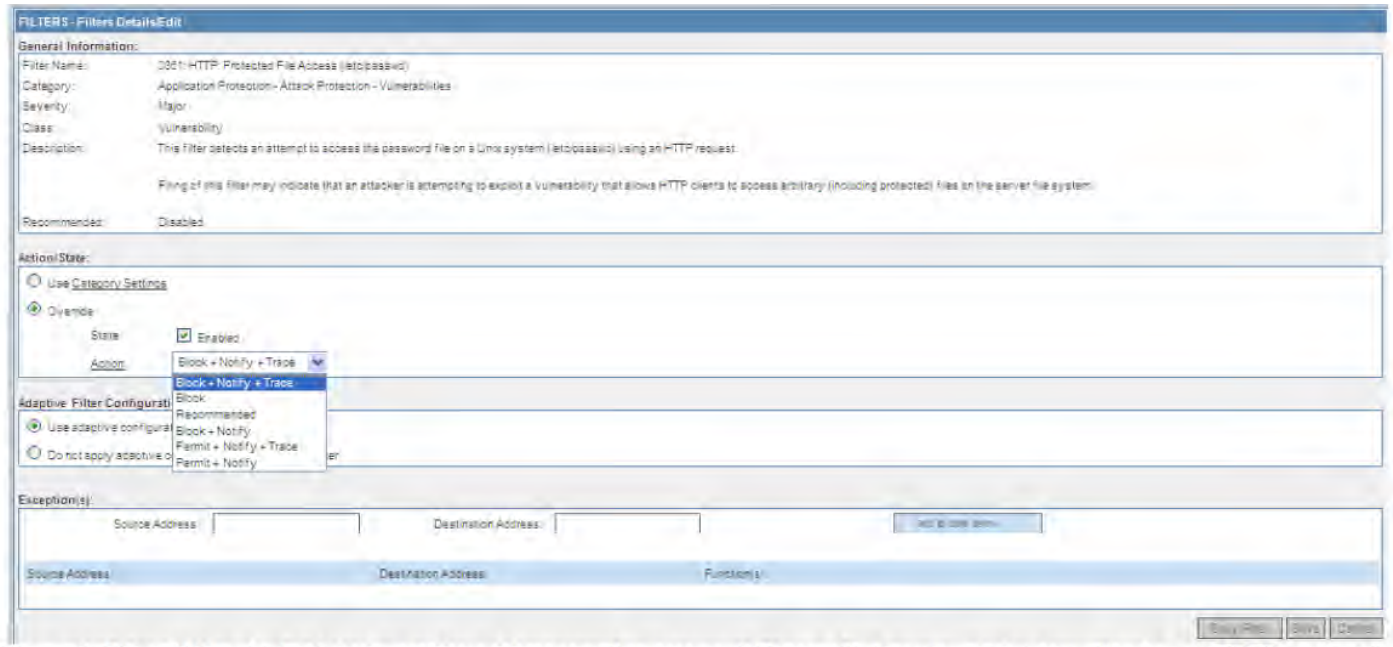
First << >> Last

1 - 600 of 1888

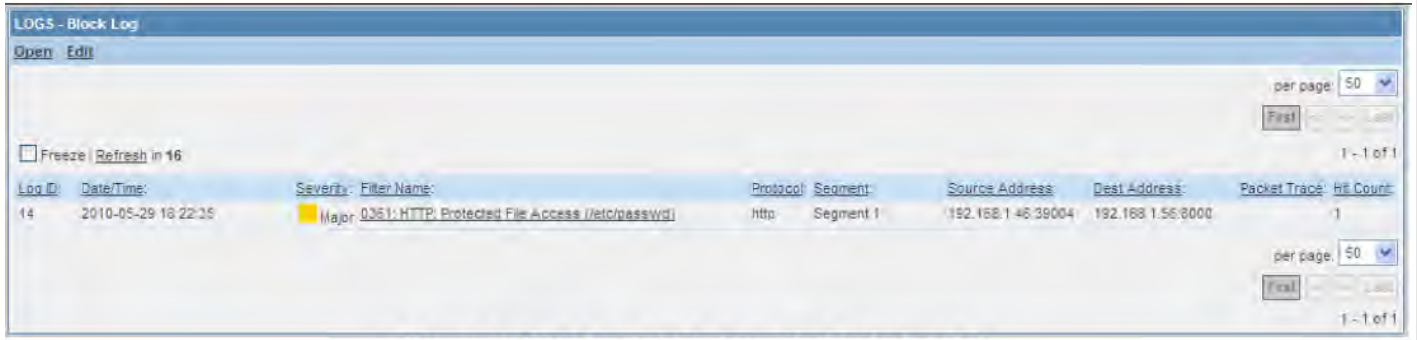
Filter Name	Segment	Control	Action	State	Function(s)
0027: IP Options: Record Route (RR)	any	Category Settings	Disabled		
0032: IP Options: Time Stamp (TS)	any	Category Settings	Disabled		
0034: IP Options: Security (SEC)	any	Category Settings	Disabled		
0035: IP Options: Loose Source Route (LSR)	any	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 5: Sample filters available in the IPS.

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **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.**

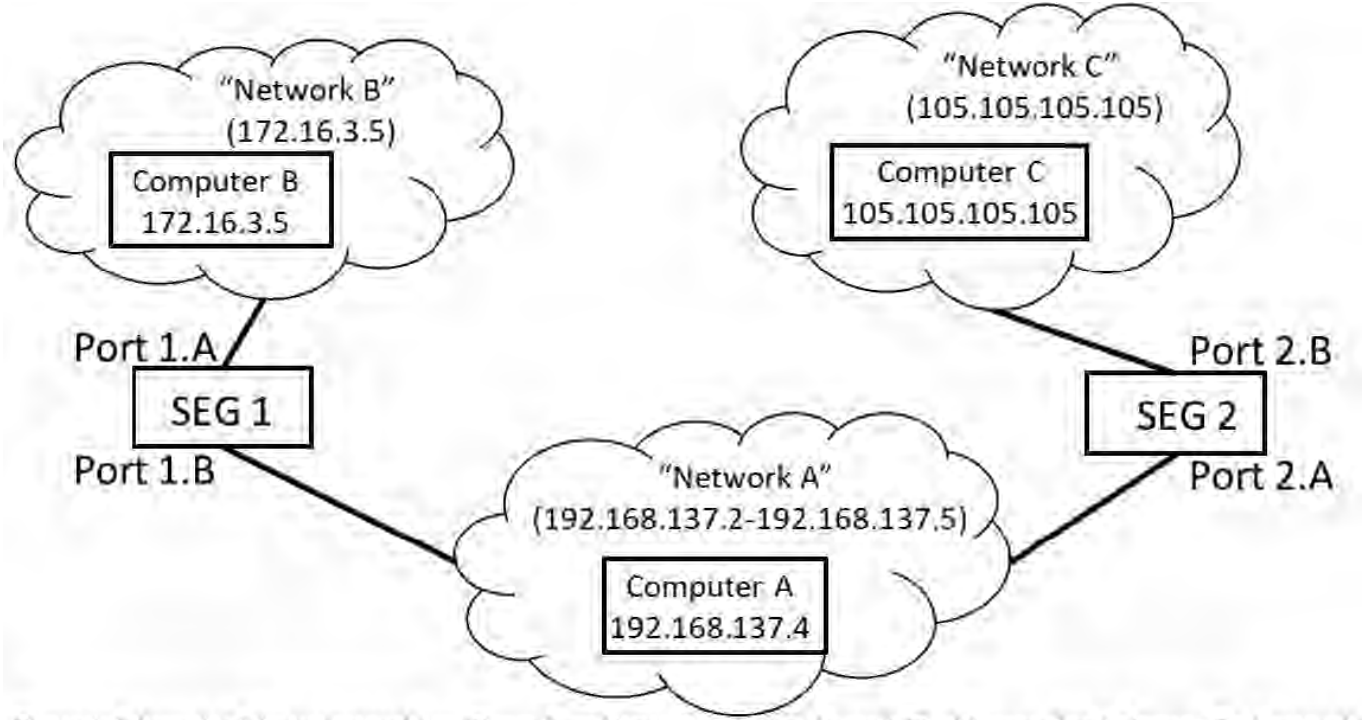
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1. **[a]** 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;	 **Figure 7: Block Log, which shows the blocked packets.**

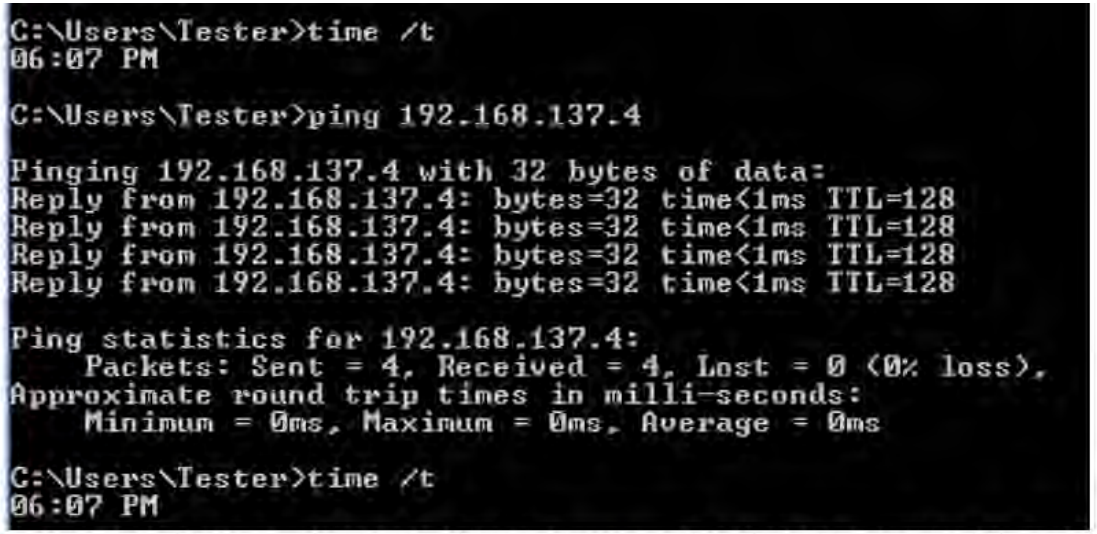
TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. **[a]** 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[b]** receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	 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.

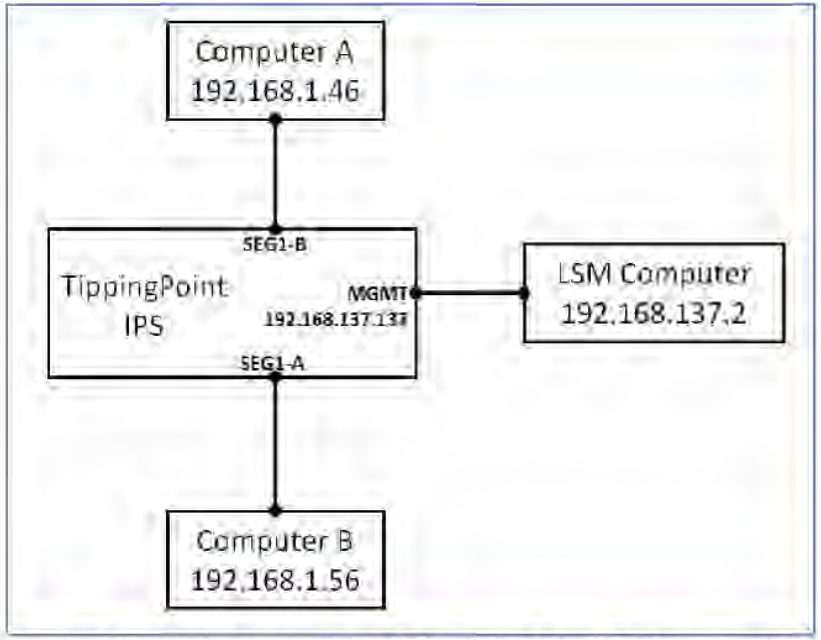
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[b]** receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	 **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.**

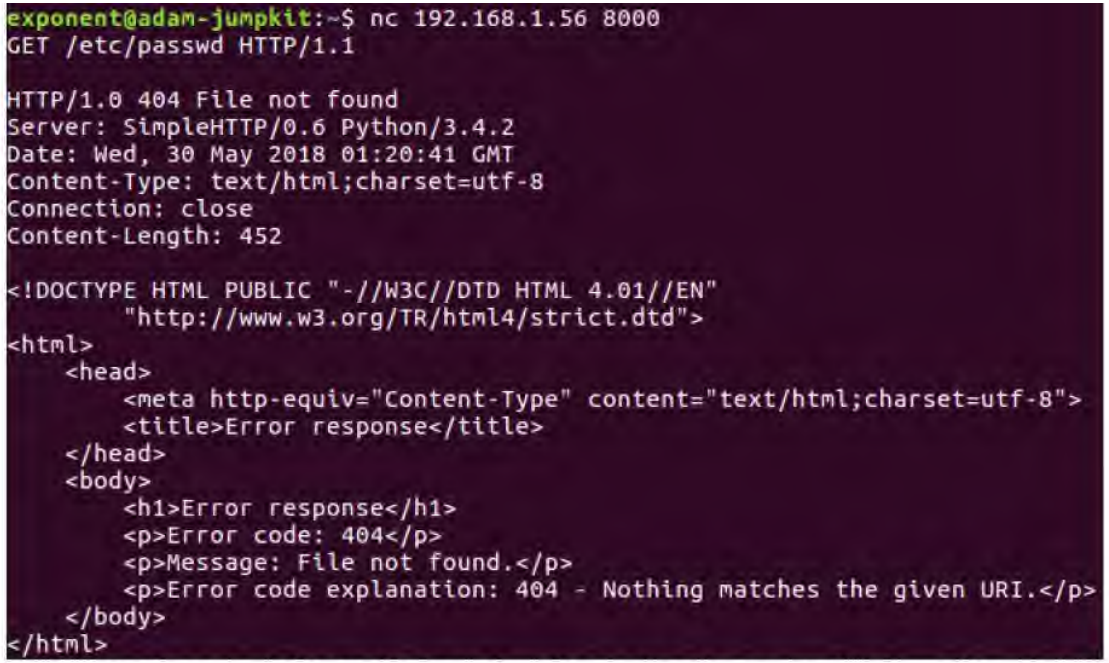
TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[c]** 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;	 Figure 9: Network map of test network illustrating connectivity of the TippingPoint IPS, Computer A, Computer B, and the LSM Computer.

’213 Patent Analysis – TippingPoint IPS

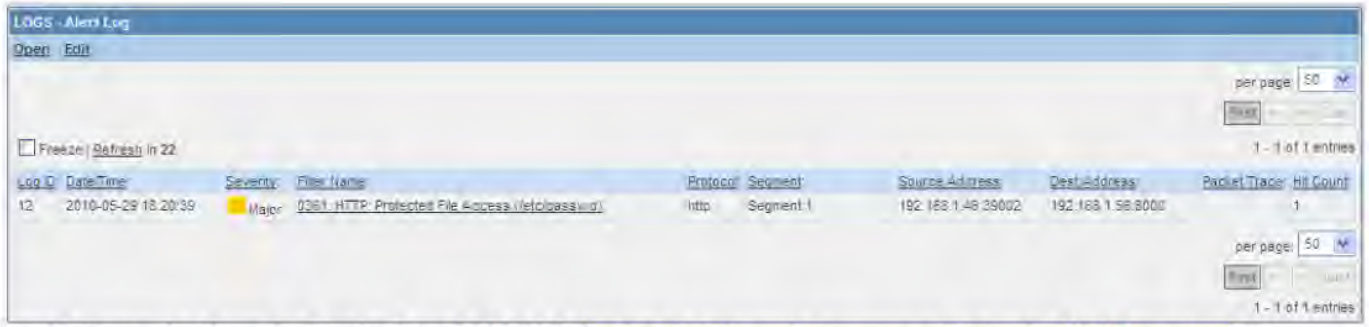
’722 Patent:	TippingPoint:
1… [c] identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information;	 **Figure 10: 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).**

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[c]** 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;	 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."

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 129

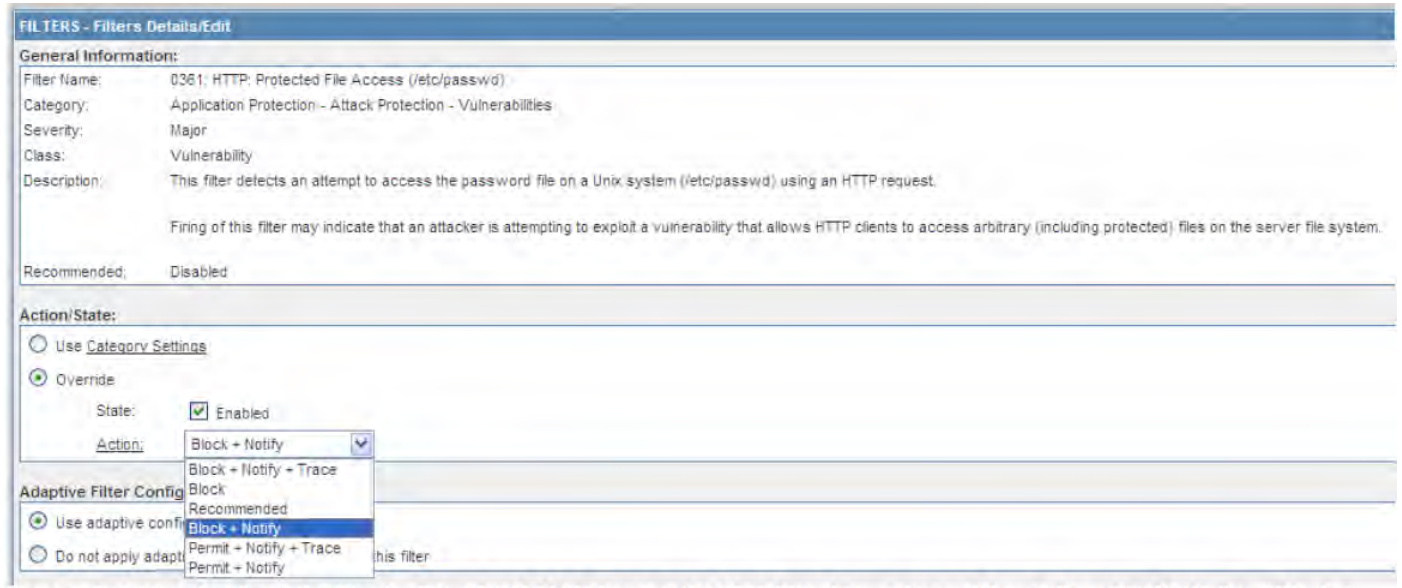
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[c]** 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;	 **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.**

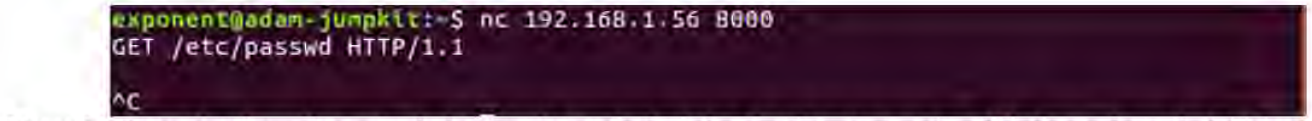
TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. **[a]** 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

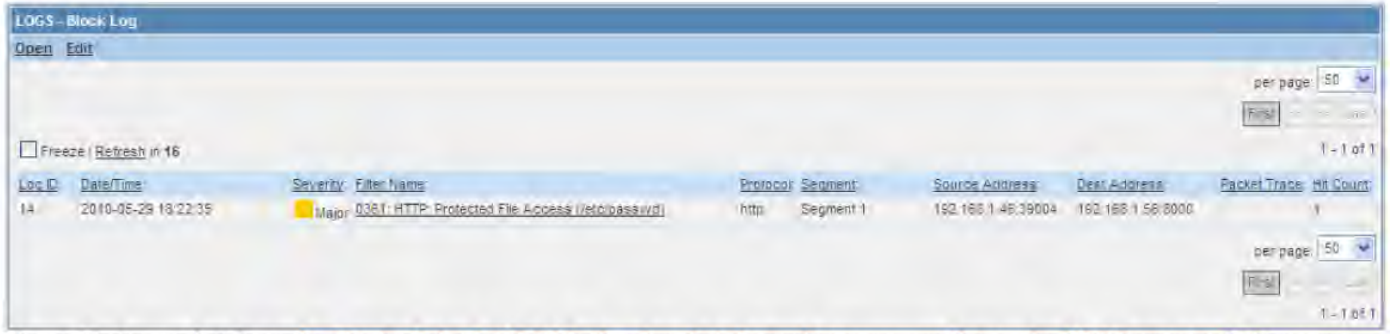
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… [d] 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	 **Figure 13: Screenshot from the TippingPoint LSM GUI showing the 0361 filter being changed from “Permit + Notify” to “Block + Notify.”**

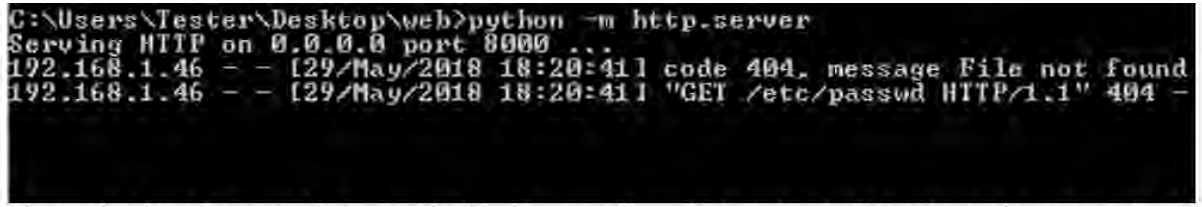
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[d]** 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	 **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).**

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[d]** 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	 **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.**

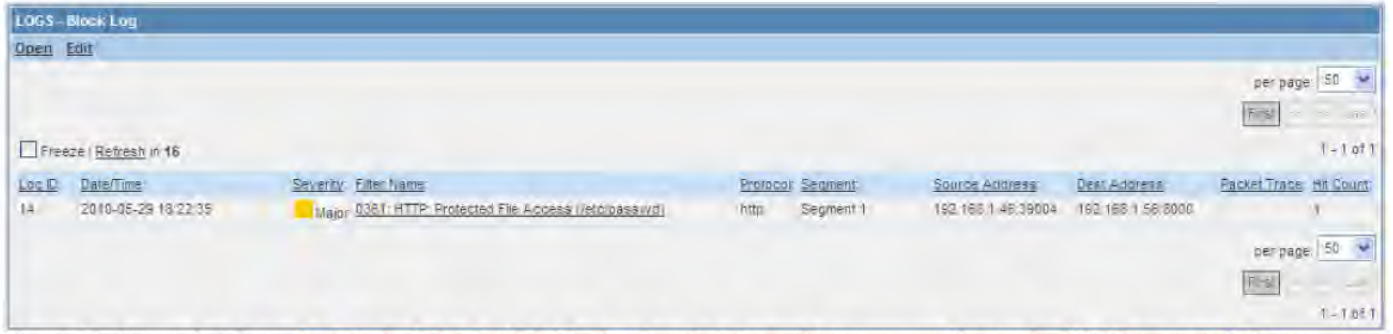
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[d]** 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	 **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.)**

TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

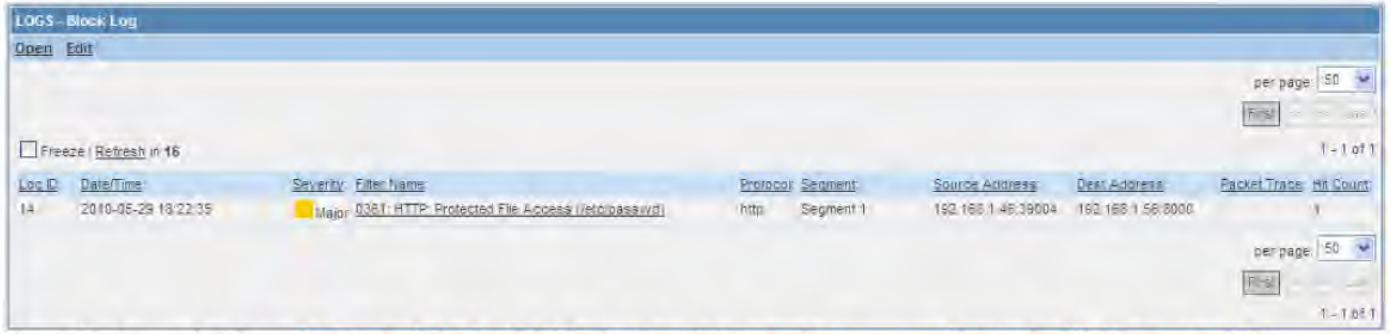
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… [e] 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;	 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.

TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	✓
[f] 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	
[g] 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	
[h] 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.	

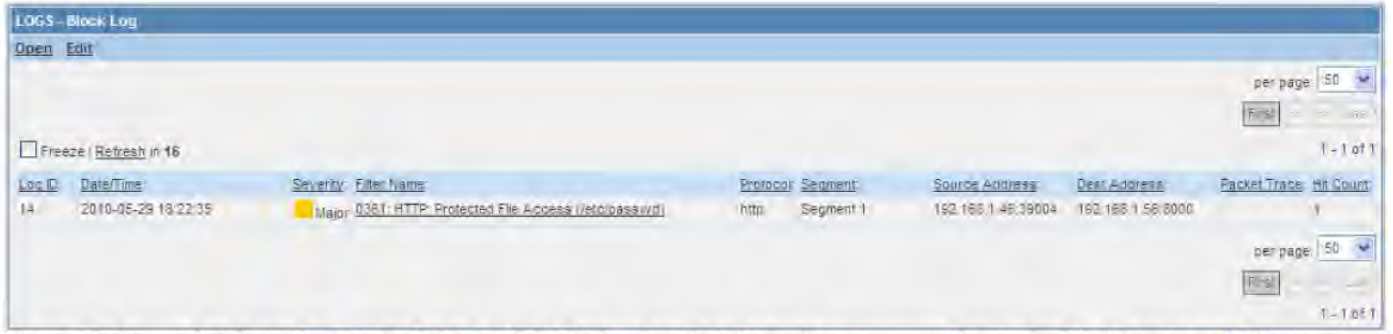
’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… [f] 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	 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.

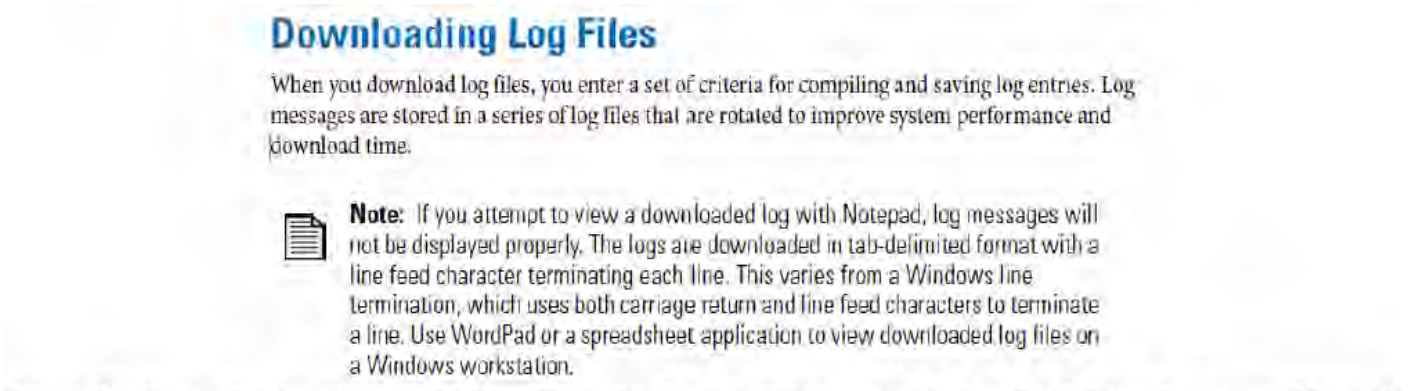
TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	✓
[f] 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	✓
[g] 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	
[h] 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.	

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… [g] 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	 **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.**

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… [g] 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	

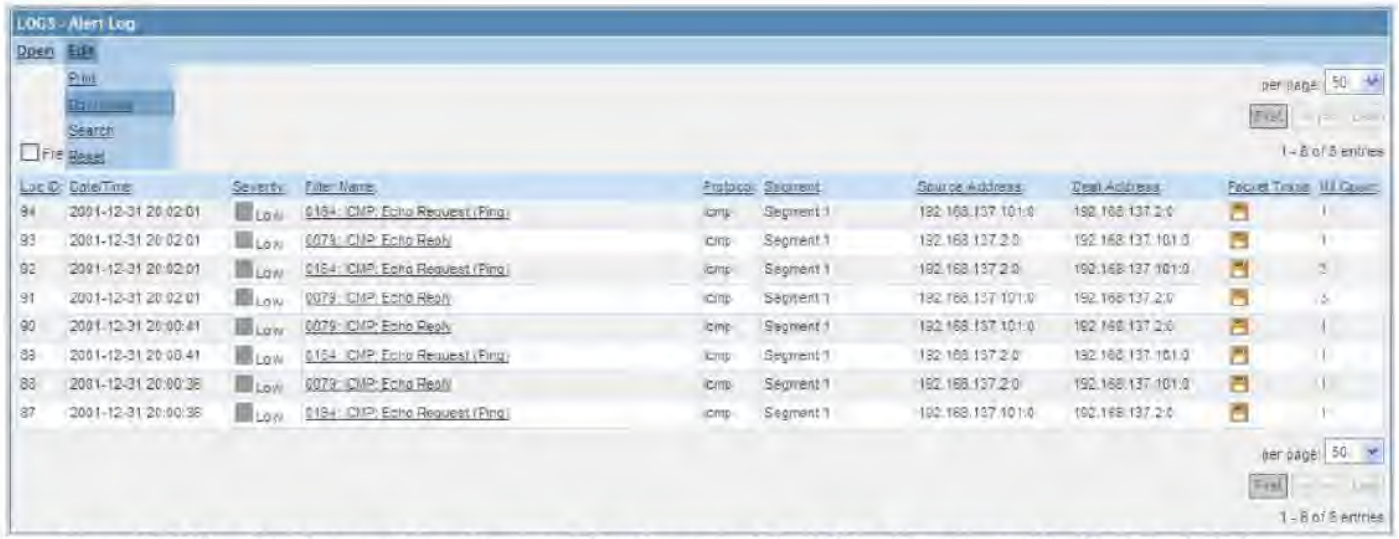
Downloading Log Files

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.

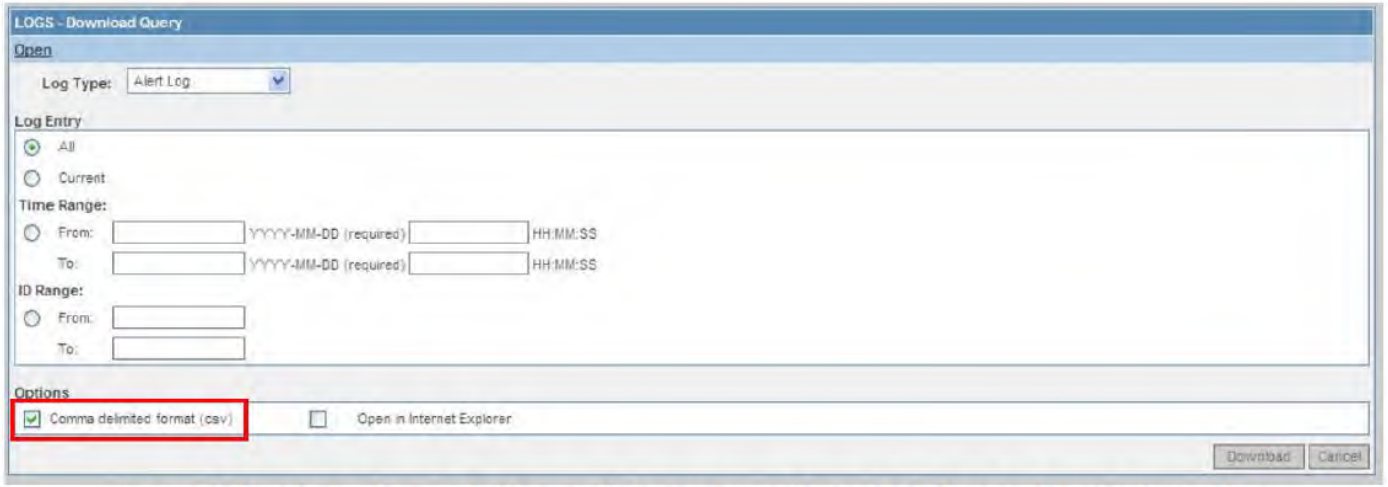
Note: If you attempt to view a downloaded log with Notepad, log messages will not be displayed properly. The logs are downloaded in tab-delimited format with a line feed character terminating each line. This varies from a Windows line termination, which uses both carriage return and line feed characters 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.

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… [g] 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	 **Figure 18: A log of packets sent from Computer B to Computer A, including the option to download (in the Edit menu).**

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… [g] 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	 **Figure 19: Download options, including specific time ranges and an option to download a .csv formatted log.**

’213 Patent Analysis – TippingPoint IPS

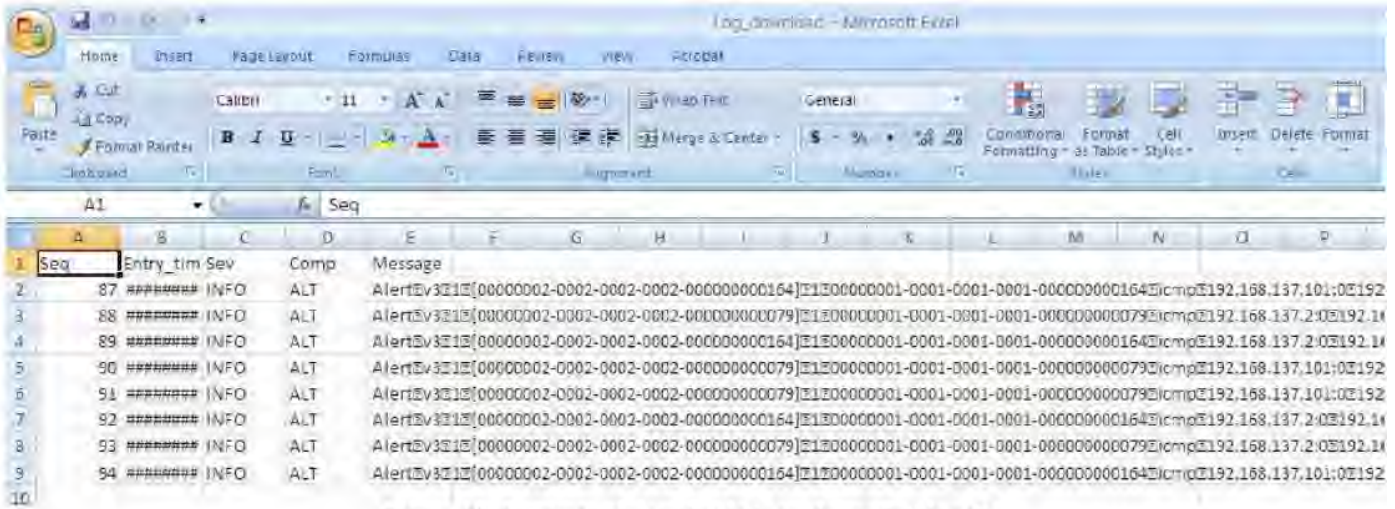
’722 Patent:	TippingPoint:
1… [g] reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and	

Figure 20: Contents of downloaded .csv formatted log file.

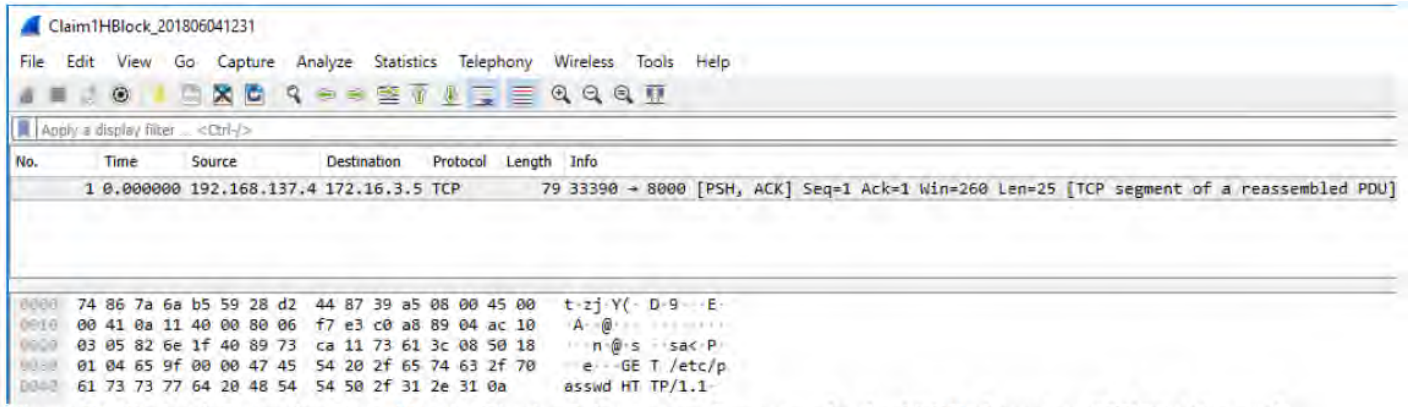
TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. [a] 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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.	

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[h]** 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.	 **Figure 21: Screenshot from the LSM GUI showing the Block Log, which lists packets that were not forwarded to their intended destination.**

’213 Patent Analysis – TippingPoint IPS

’722 Patent:	TippingPoint:
1… **[h]** 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.	 **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.**

TippingPoint IPS Invalidates the ’213 Patent, Claim 1

’213 Patent:	TippingPoint:
1. **[a]** 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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.	✓

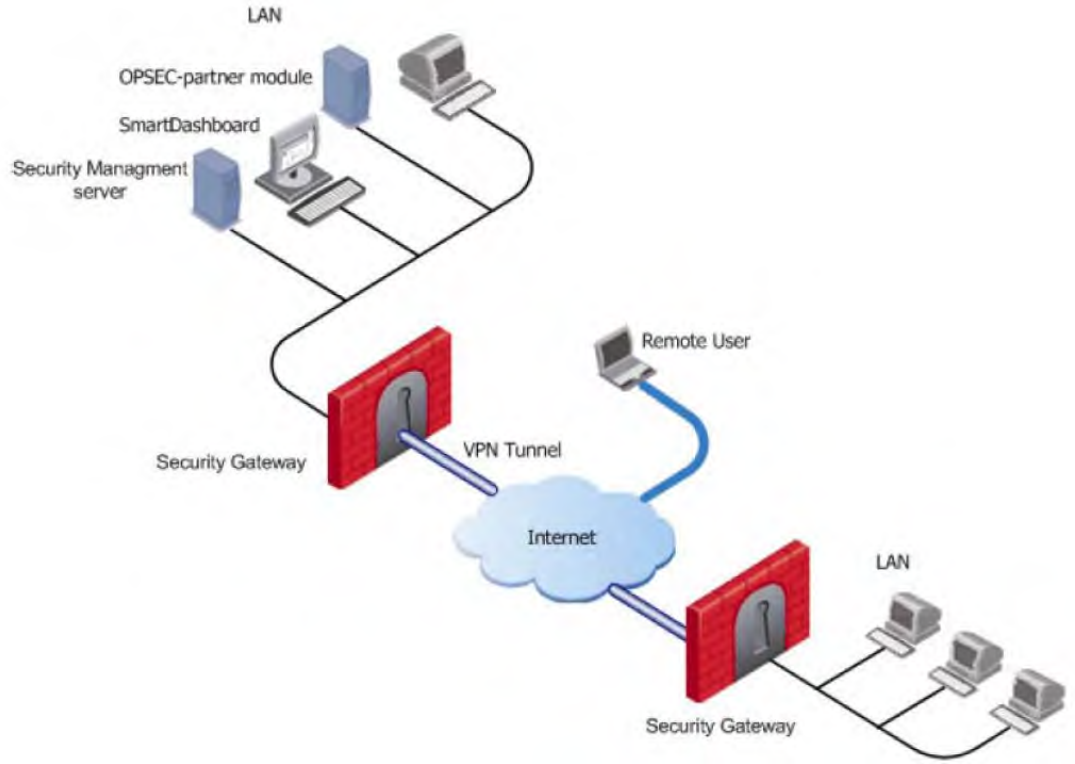

Check Point R75

Check Point R75 Invalidates the ’205 Patent Claim 17

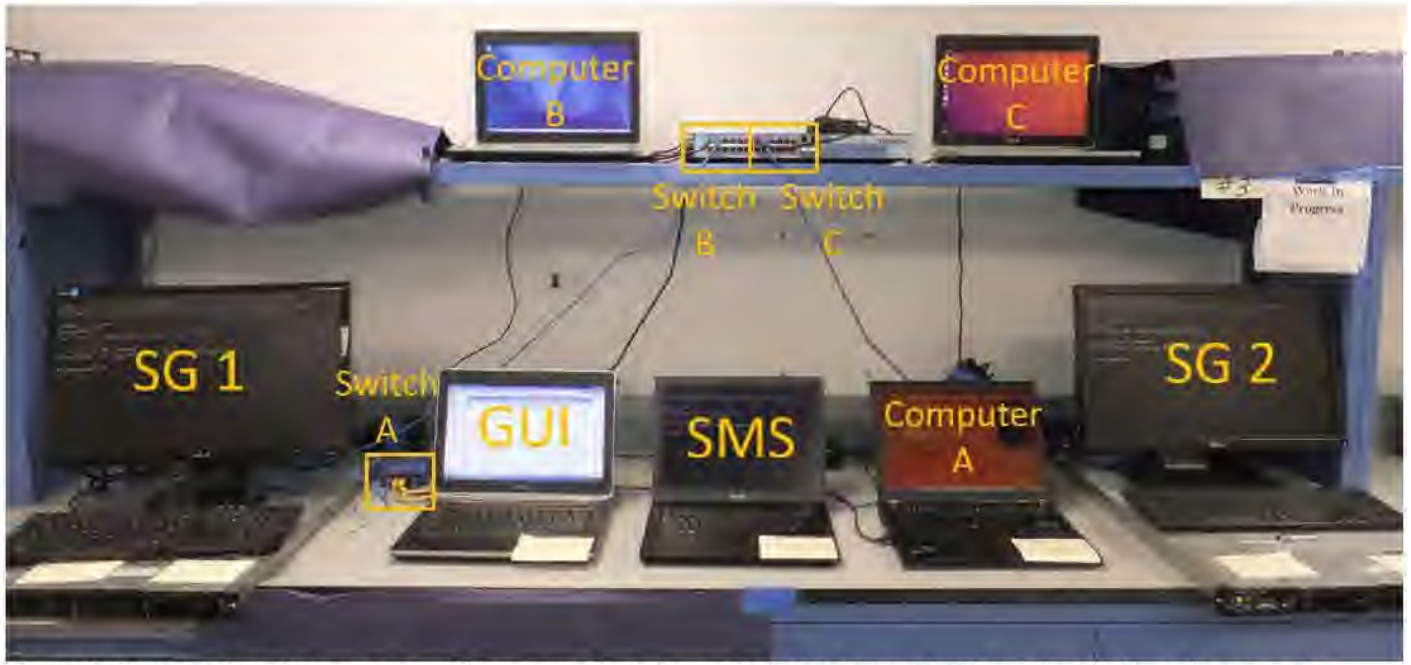
Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. [a] 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:	
[b] receive a plurality of dynamic security policies from the security policy management server,	
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

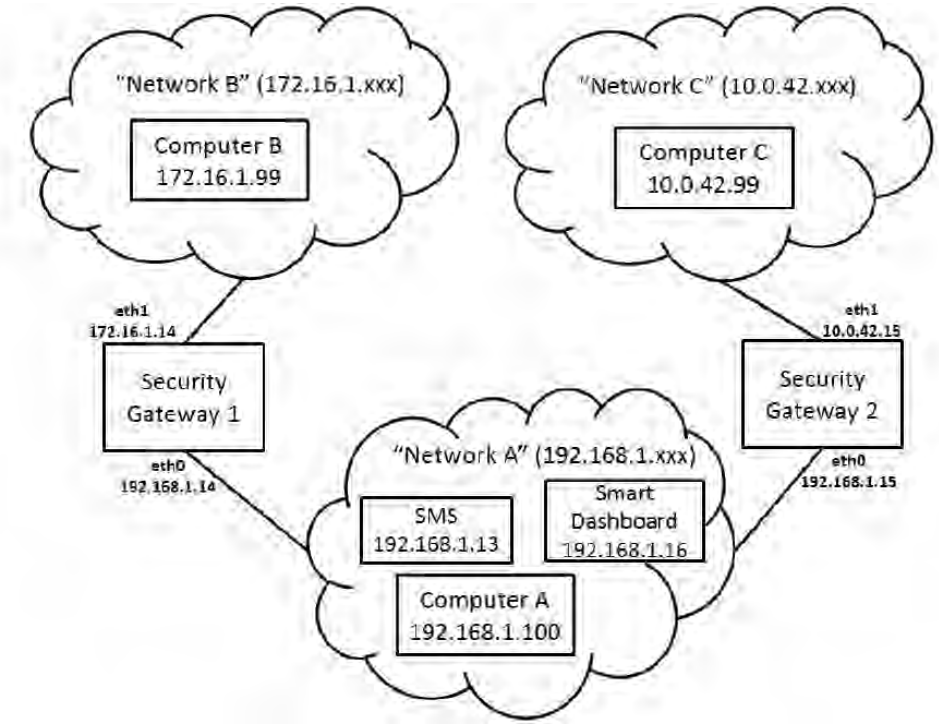
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17. [a] 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:	 **Figure 1: Illustration of a typical deployment consisting of two security gateways and a security management server (configurable using the “SmartDashboard” GUI).**[3]

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17. [a] 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:	 **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.**

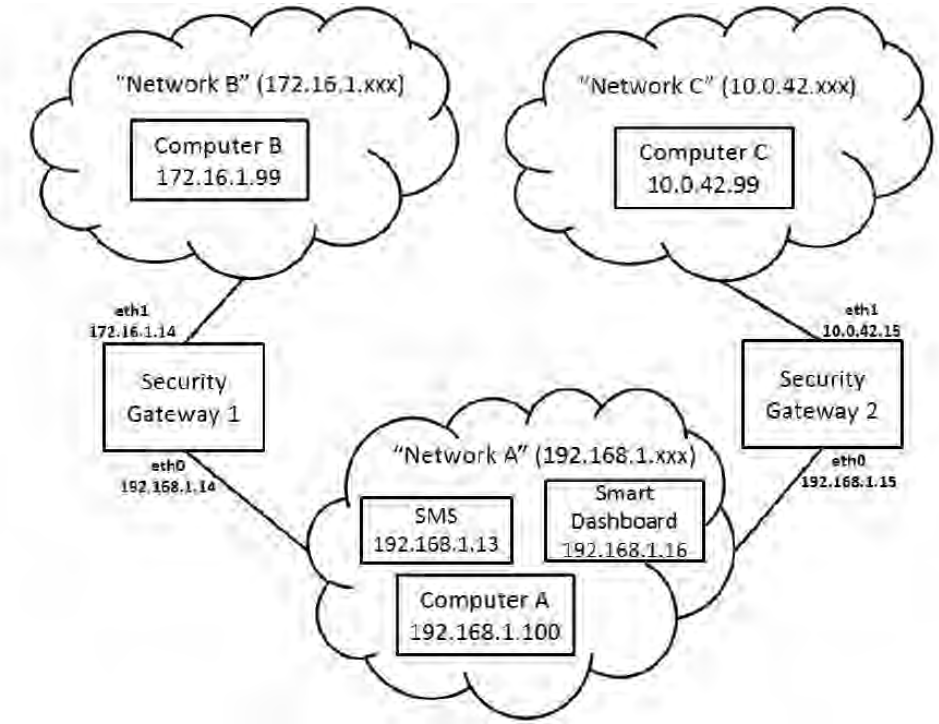
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17. [a] 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:	 **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.**

Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. **[a]** 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

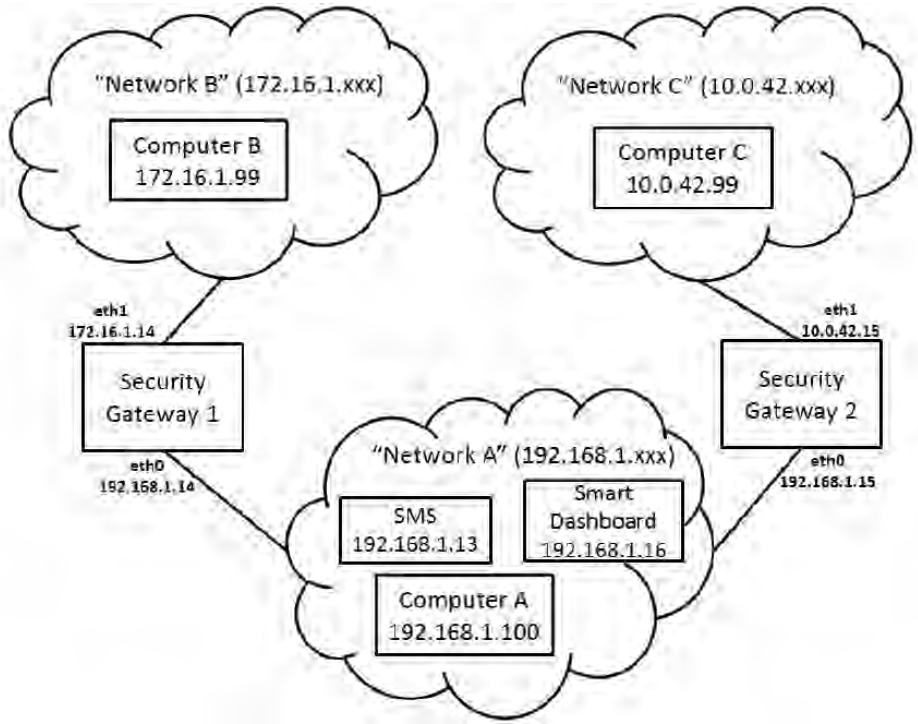
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[b]** receive a plurality of dynamic security policies from the security policy management server,	 **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.**

Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. **[a]** 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[c]** 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;	 **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.**

’205 Patent Analysis – Check Point R75

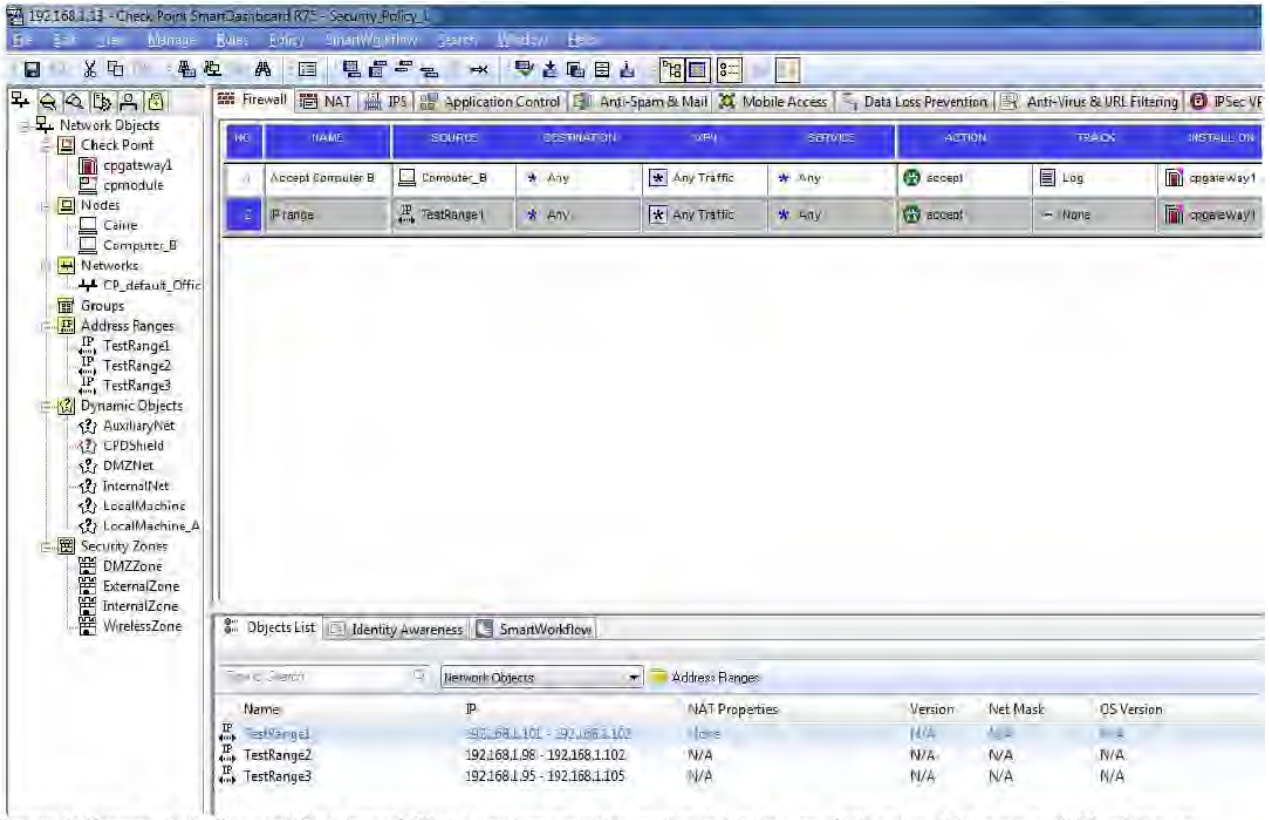
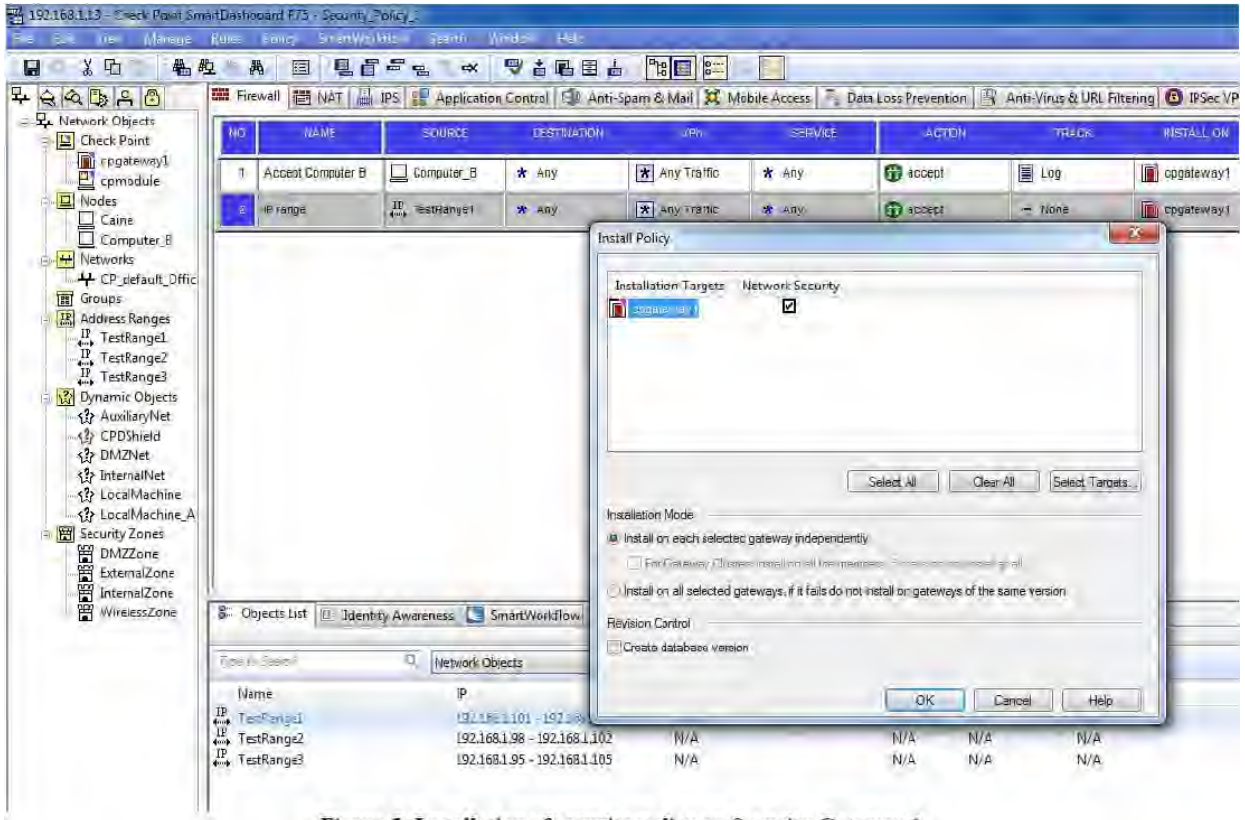
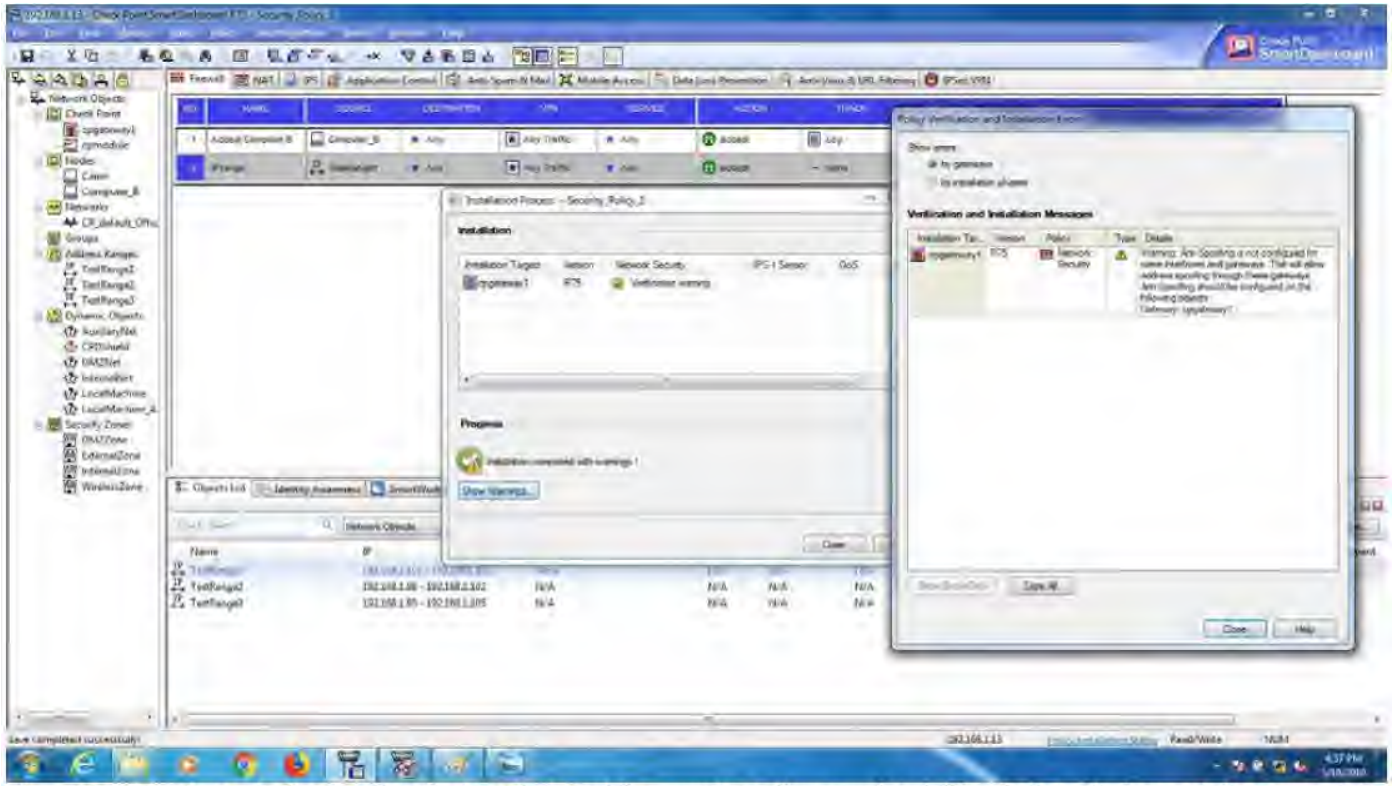
’205 Patent:	Check Point R75
17… [c] receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;	

Figure 4: Screenshot of SmartDashboard GUI showing security policy with two explicit rules. The range of IP addresses

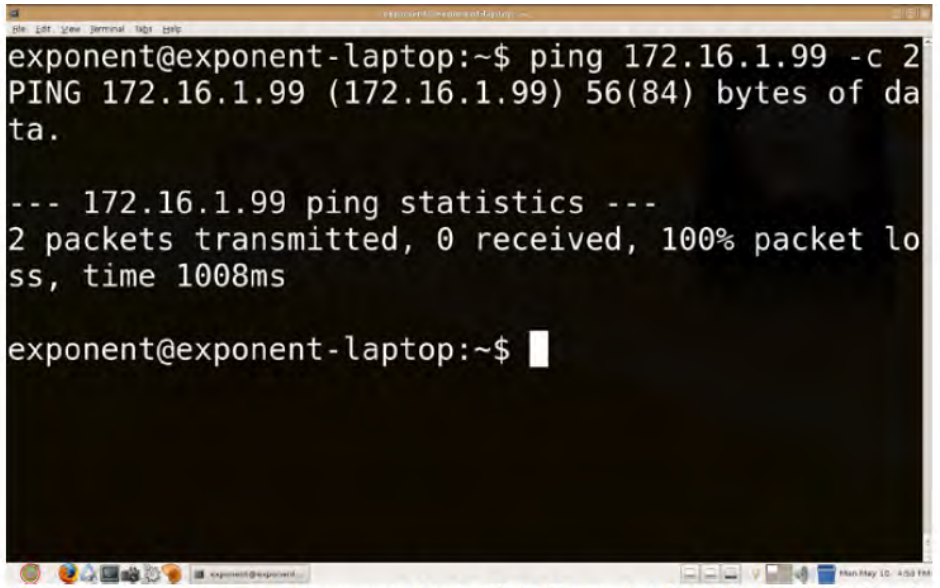
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [c] 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;	 **Figure 5: Installation of security policy on Security Gateway 1.**

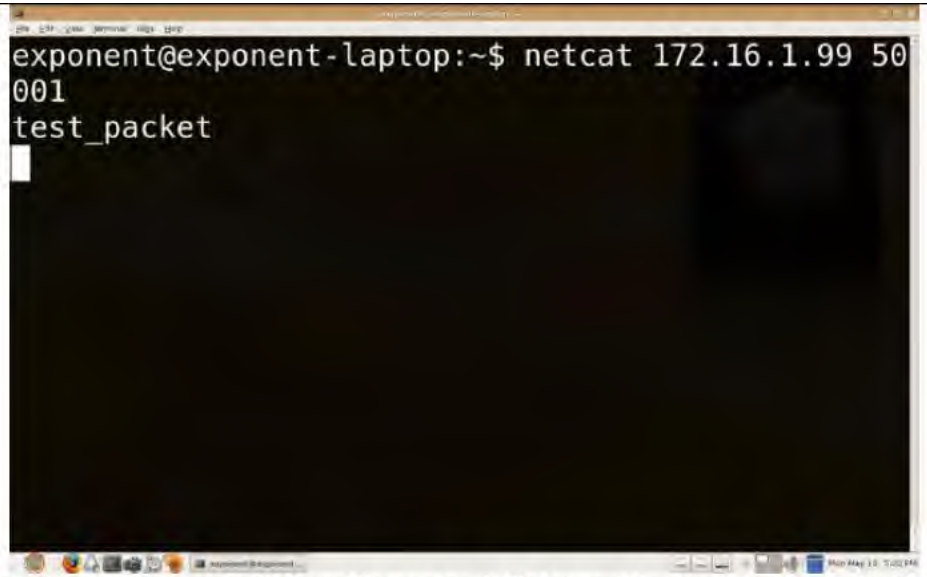
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [c] 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;	 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.

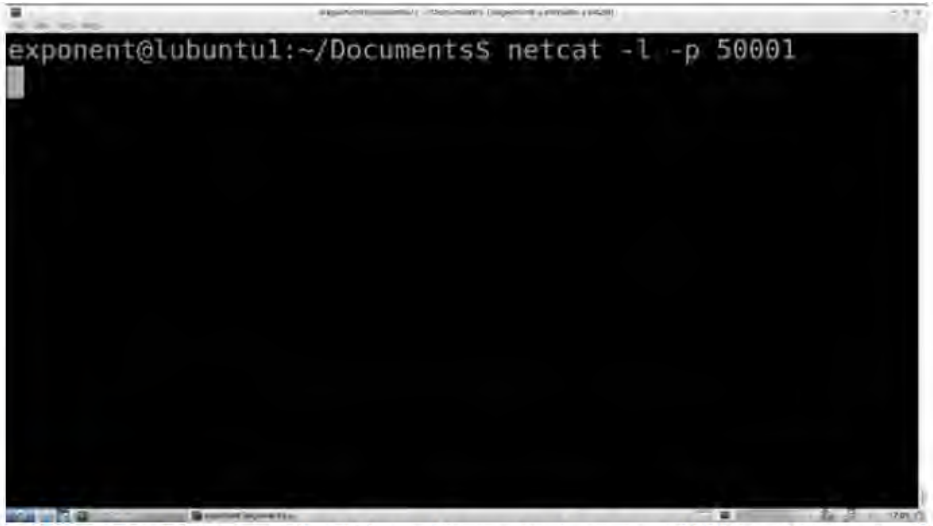
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [c] 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;	**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)  **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.**

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [c] 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;	 **Figure 8: Sending packet of text (“test_packet”) from Computer A (“exponent-laptop”) to Computer B (172.16.1.99) on port 50001.**

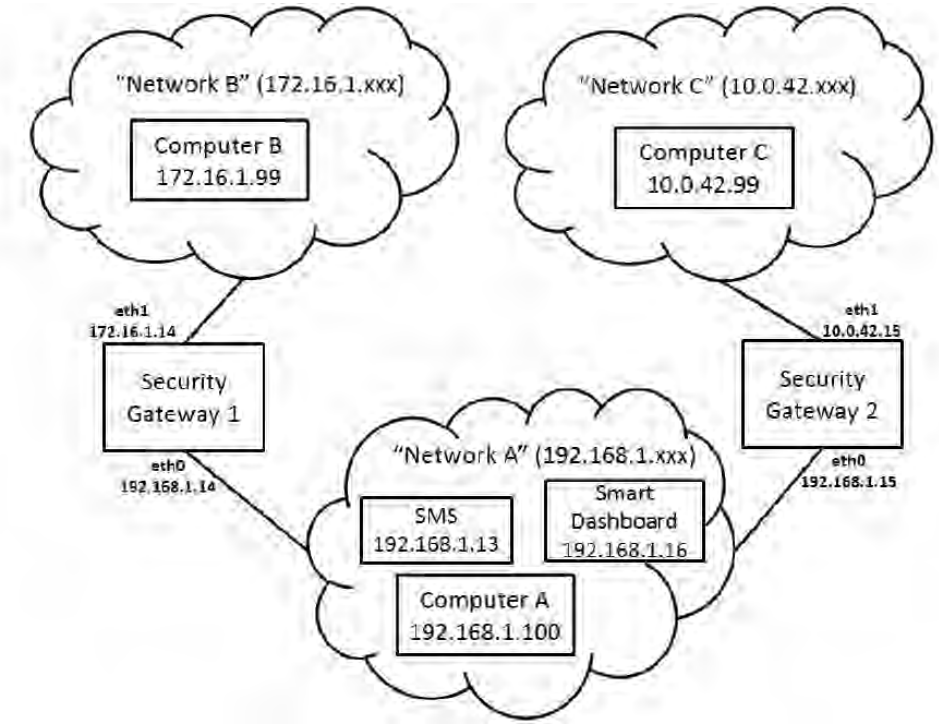
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [c] 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;	 **Figure 9: Listening for a packet of text (“test_packet”) from Computer A on port 50001 on Computer B. No packet was received.**

Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. **[a]** 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

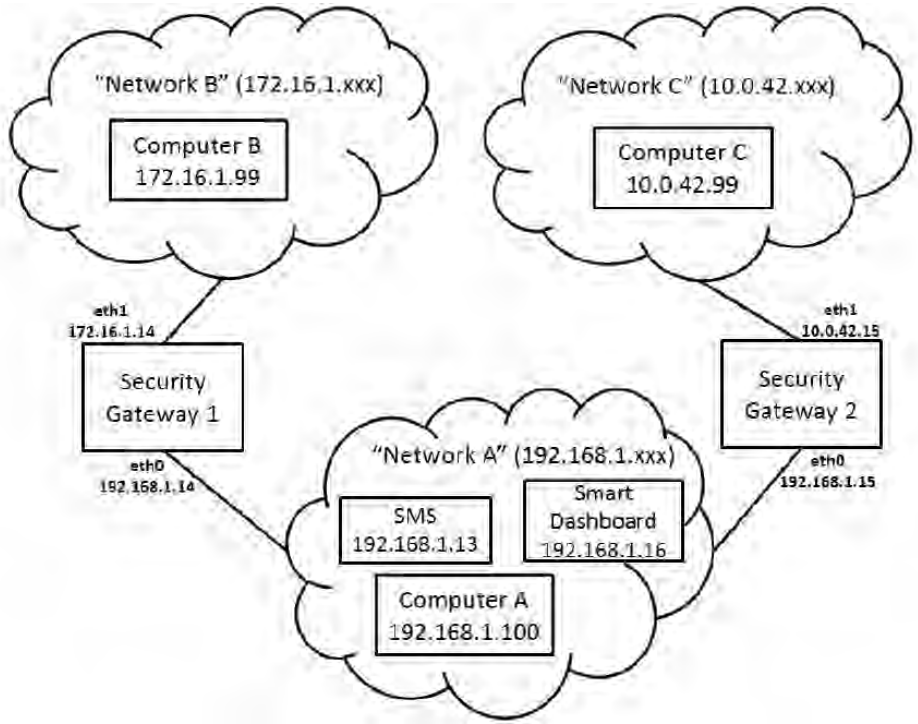
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[d]** receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	 **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.**

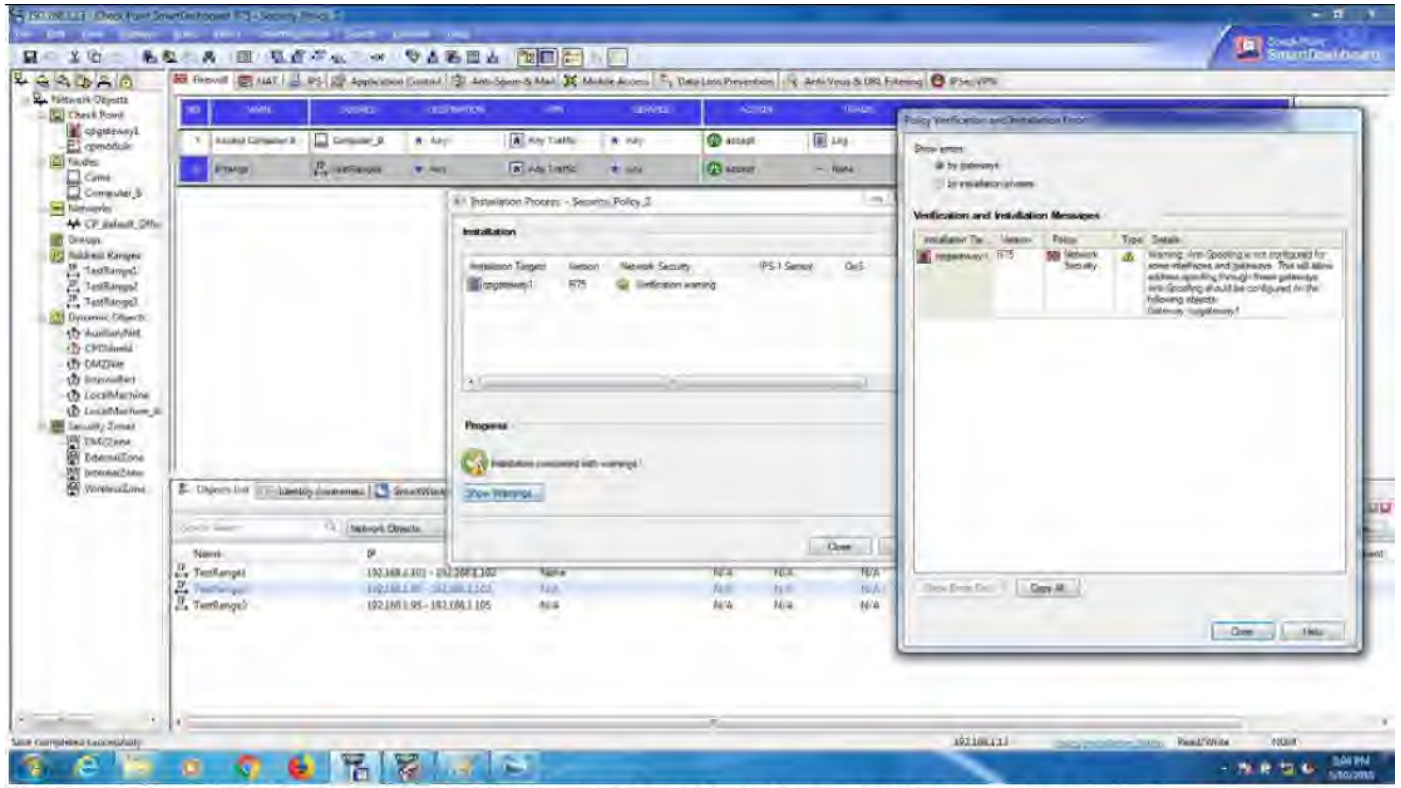
Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

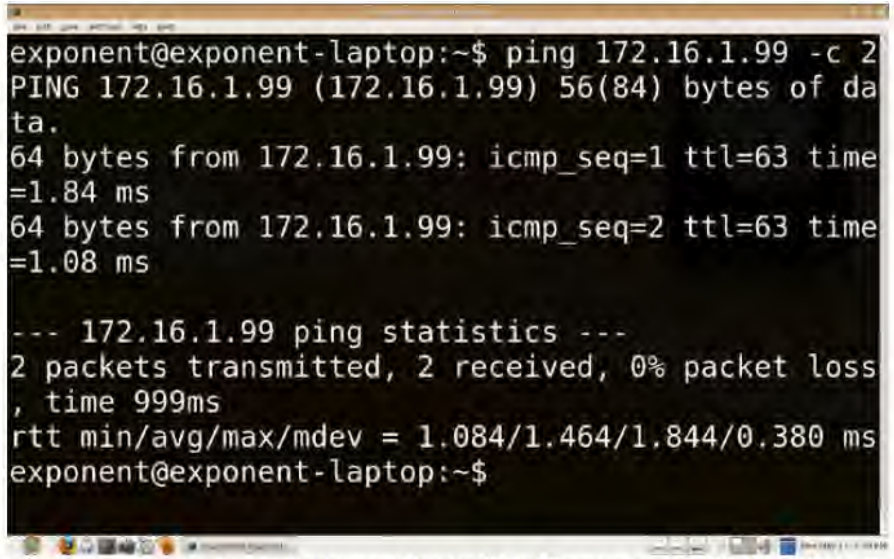
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[e]** receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	 **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.**

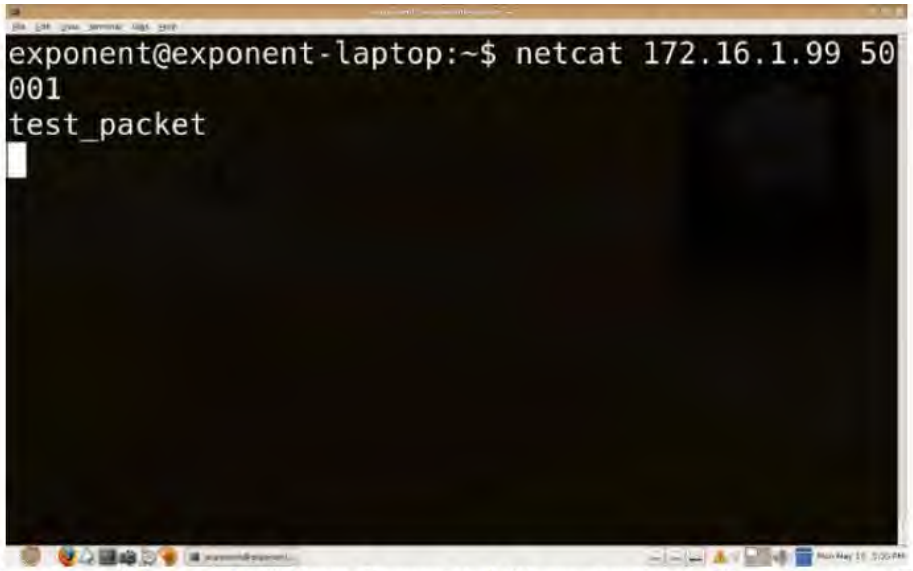
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[e]** receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	 **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.**

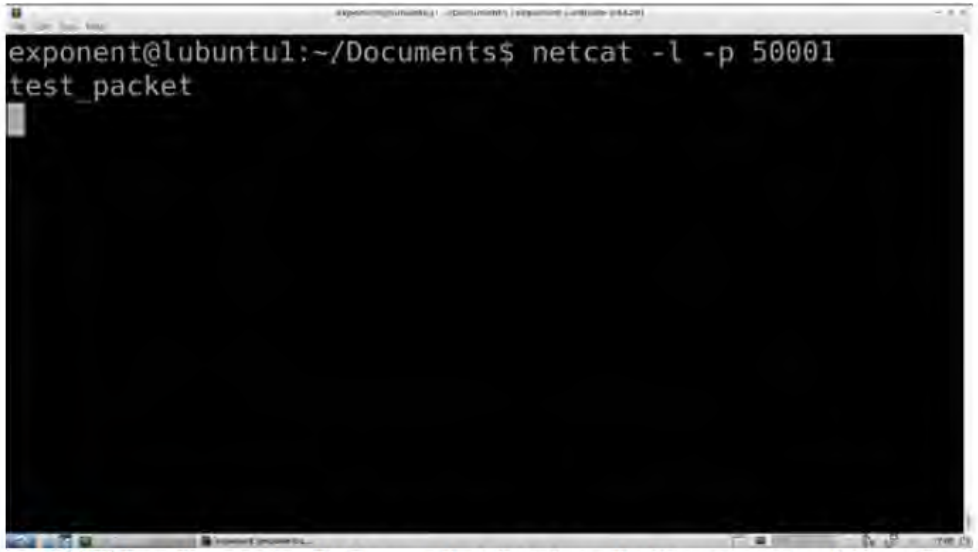
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	**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.**

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	 **Figure 12: Sending packet of text (“test_packet”) from Computer A (“exponent-laptop”) to Computer B (172.16.1.99) on port 50001.**

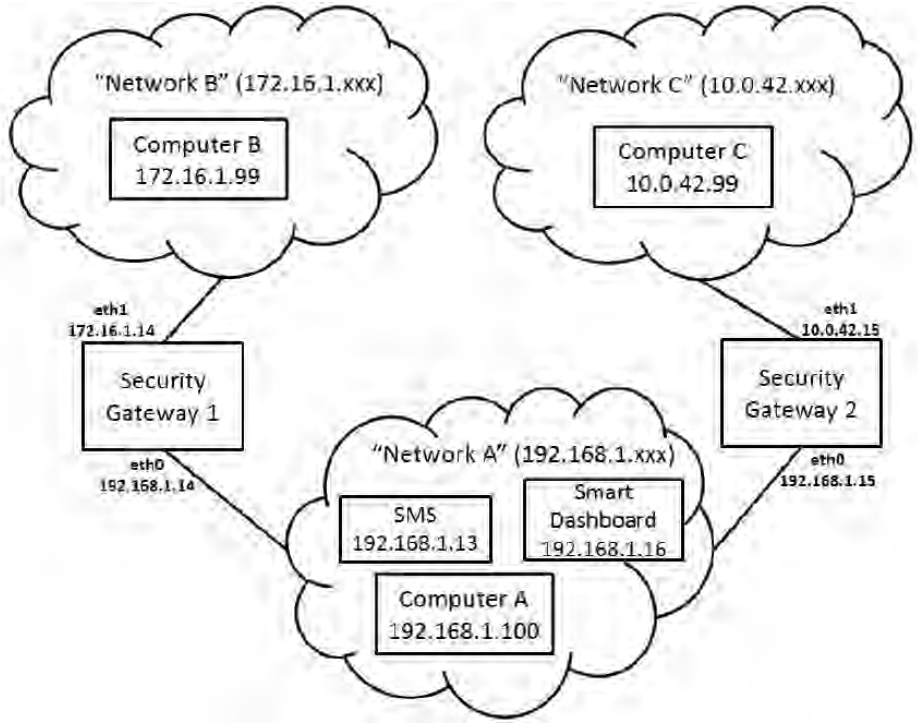
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	 **Figure 13: Listening on port 50001 on Computer B. One packet (“test_packet”) was received from Computer A.** **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)

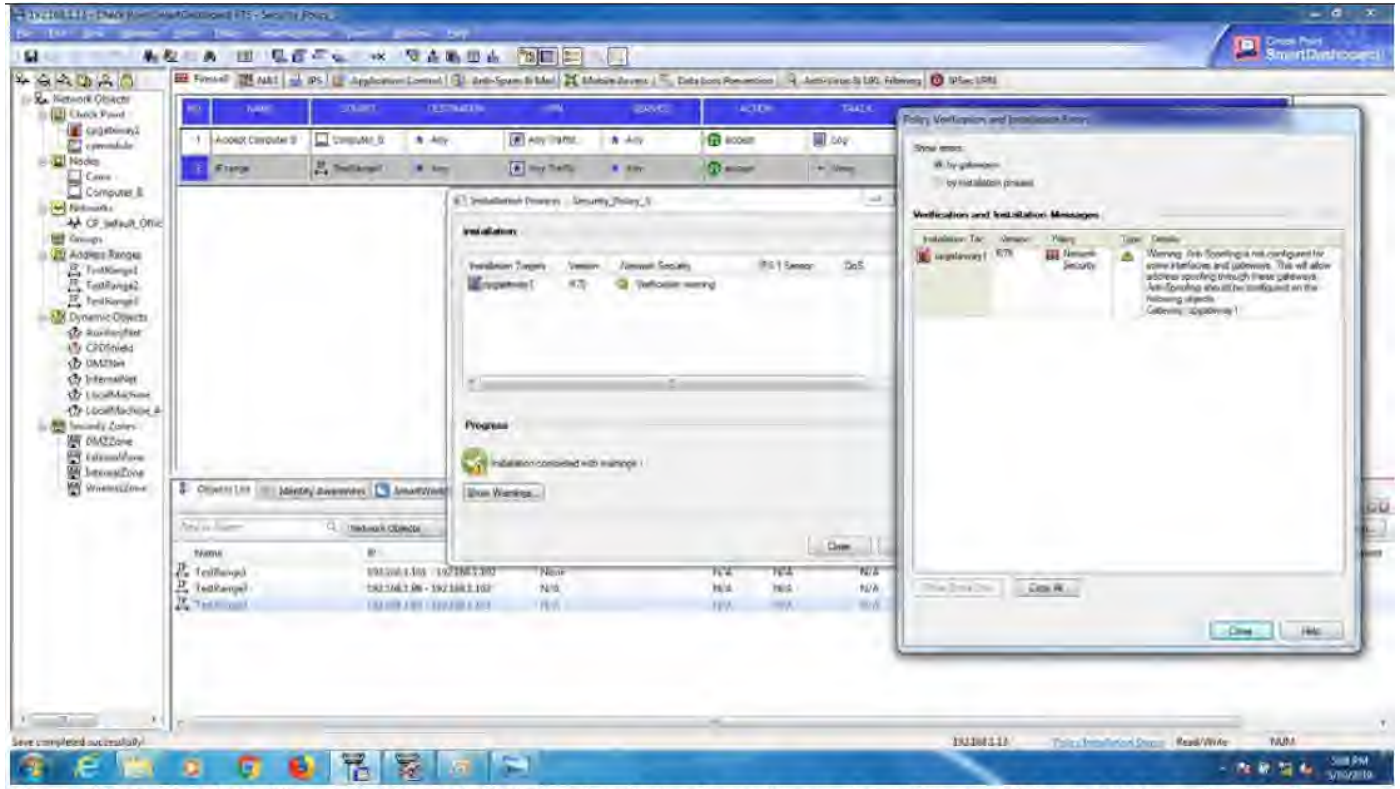
Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. **[a]** 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

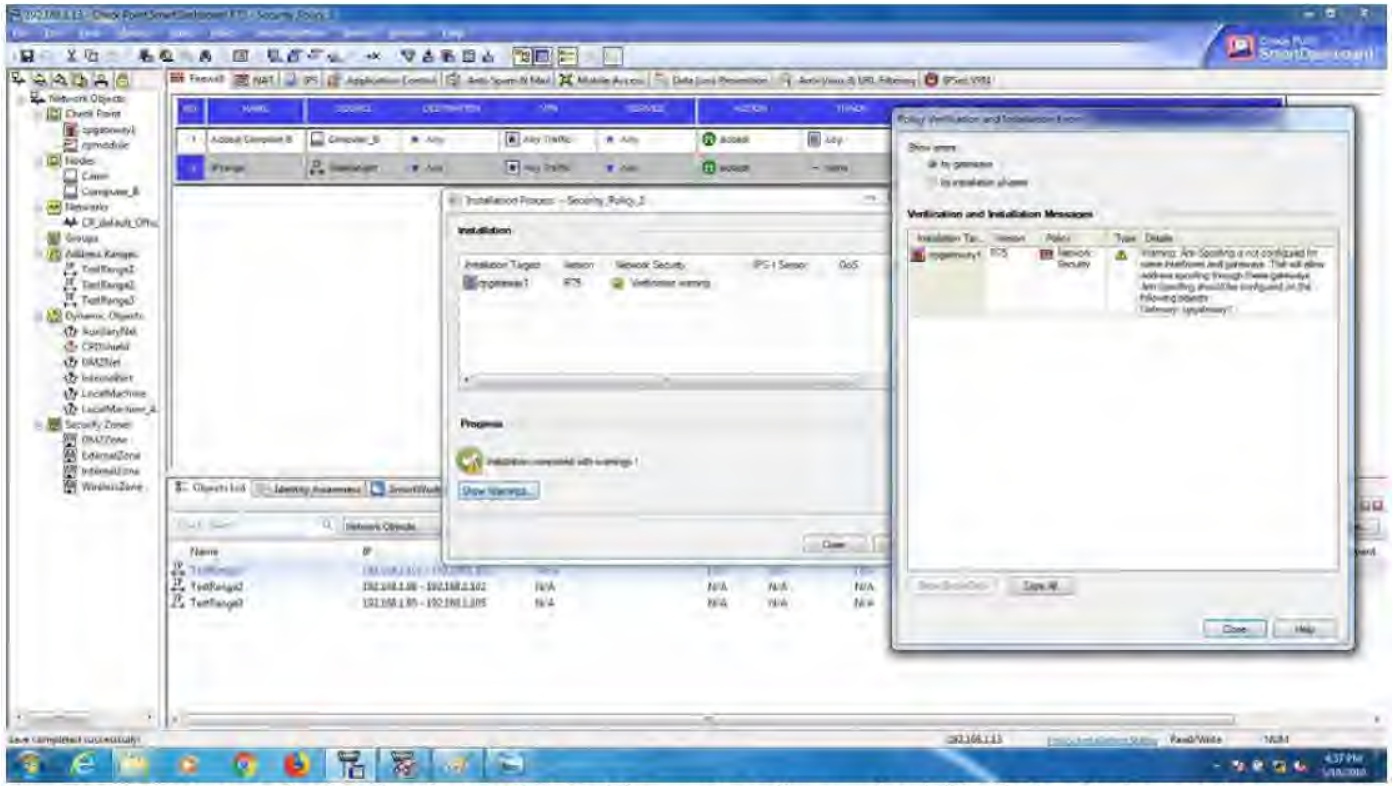
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [f] 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;	 **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.**

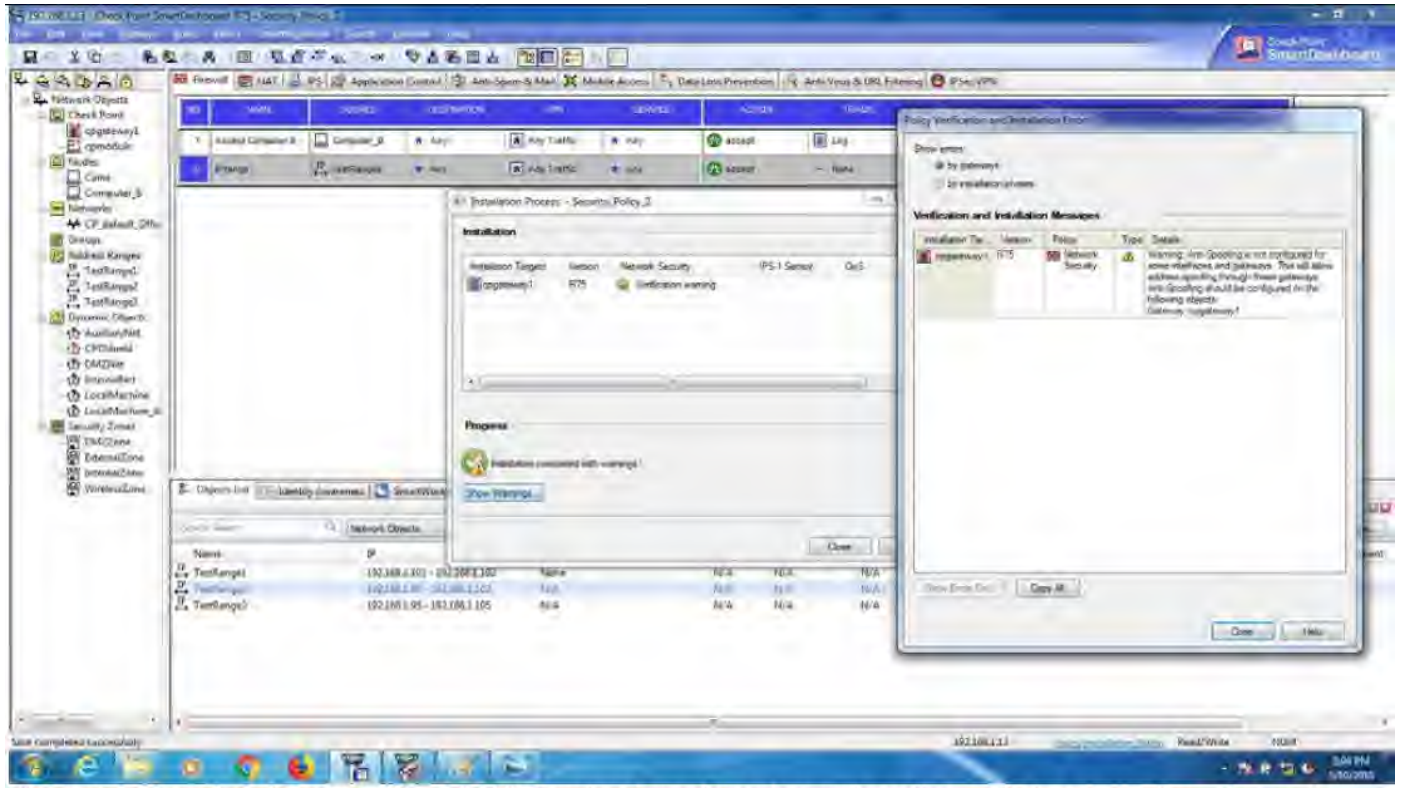
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [f] 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;	 **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.**

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [f] 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;	 **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.**

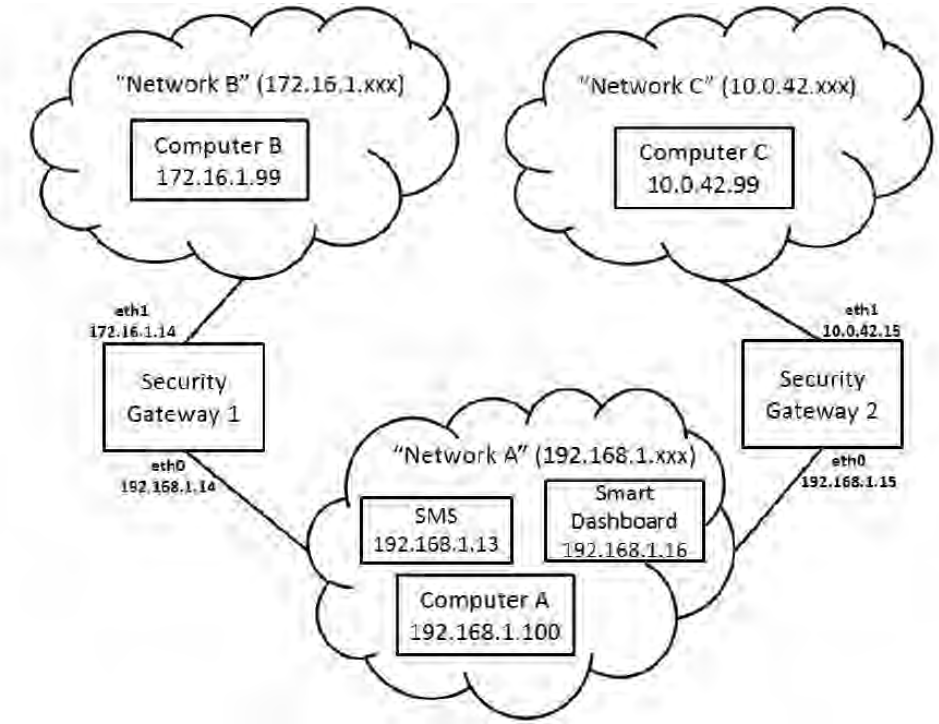
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [f] 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;	 **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.**

Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

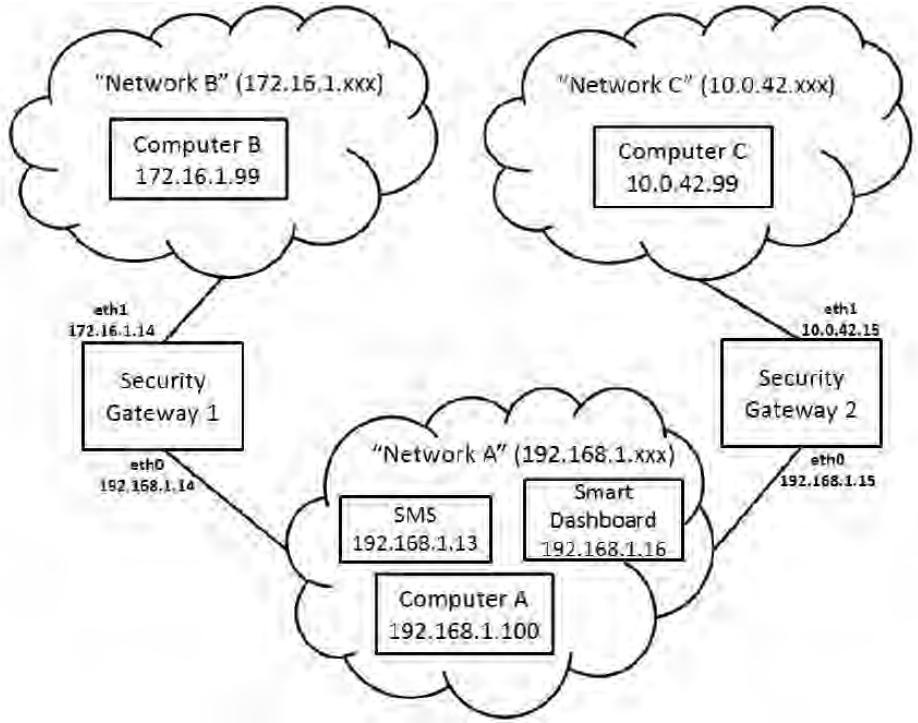
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [g] receive packets associated with a network protected by the packet security gateway; and	 **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.**

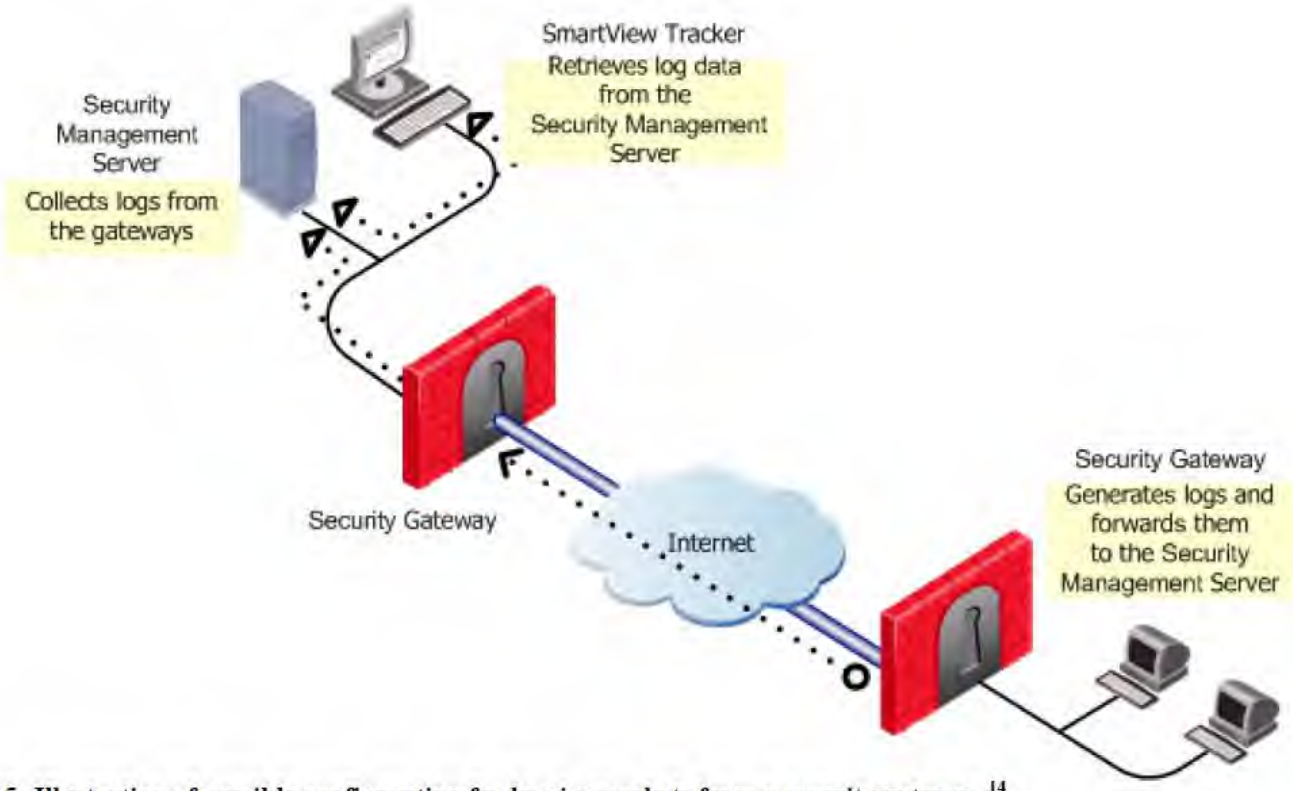
Check Point R75 Invalidates the ’205 Patent, Claim 17

’205 Patent:	Check Point R75
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	

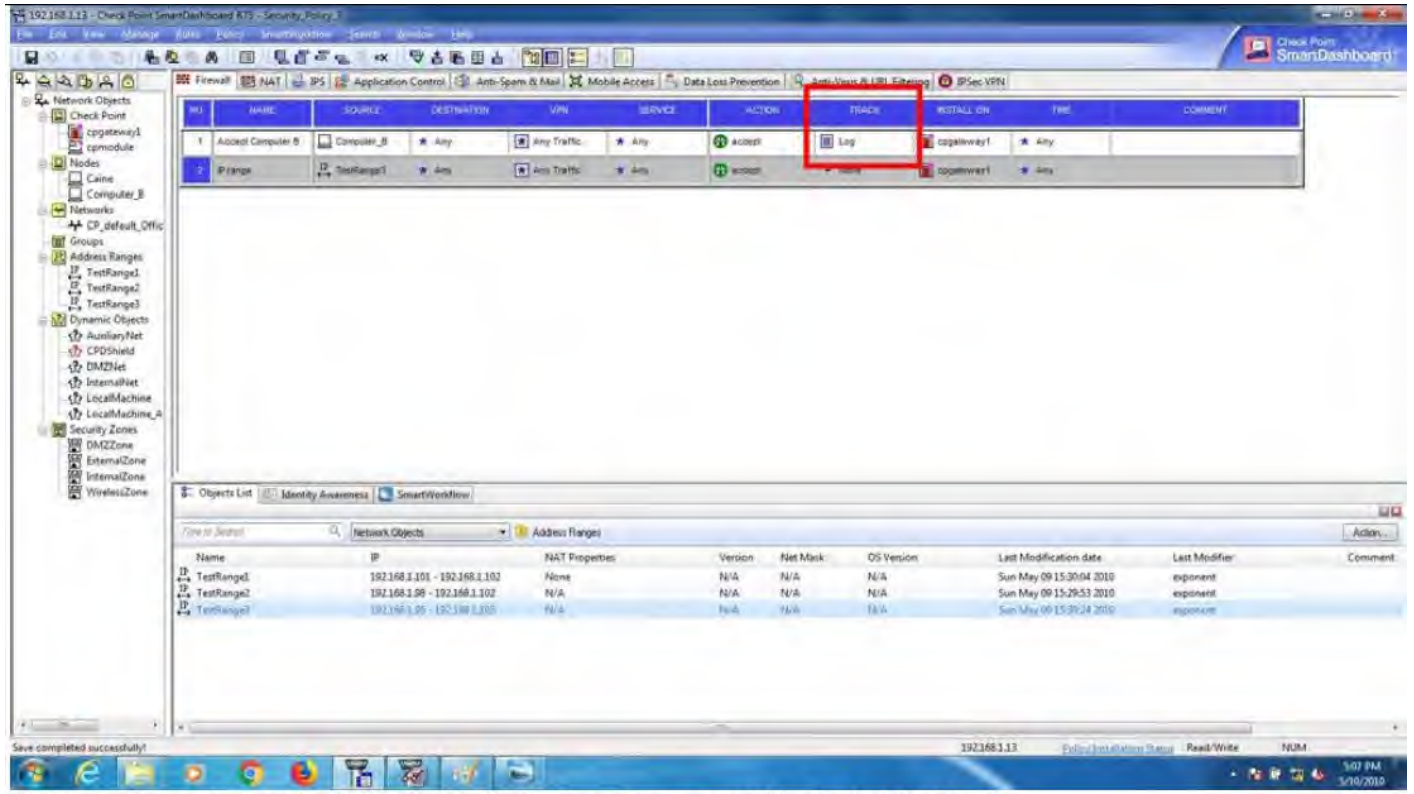
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[h]** 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.	 **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.**

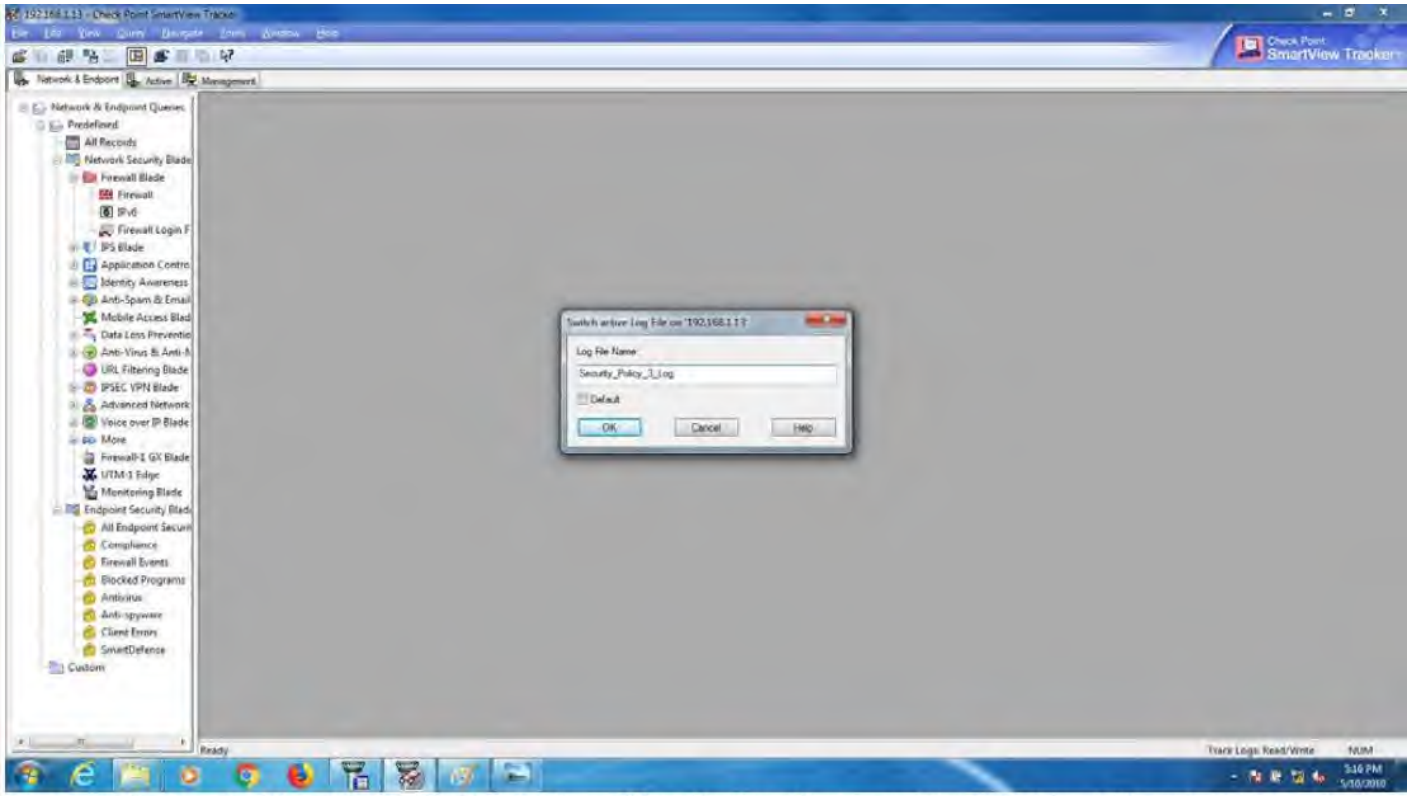
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[h]** 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.	 **Figure 15: Illustration of possible configuration for logging packets from a security gateway.**[14]

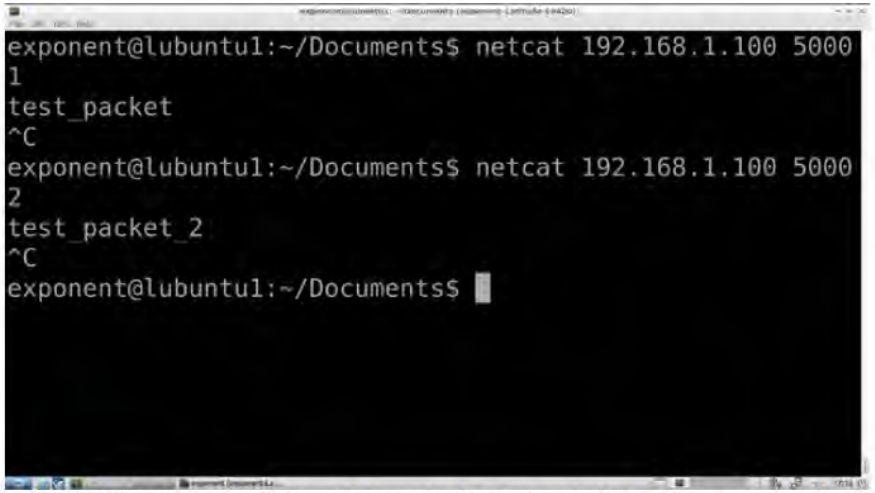
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[h]** 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.	 **Figure 16: Dynamic Security Policy 3 includes logging of events matching Rule 1 (red box).**

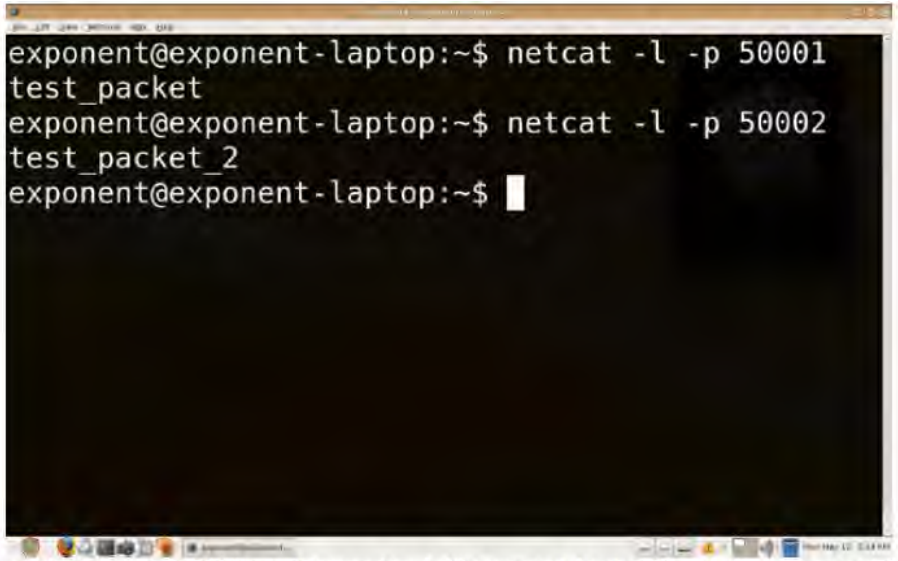
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[h]** 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.	 **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.**

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [h] 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.	 **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.**

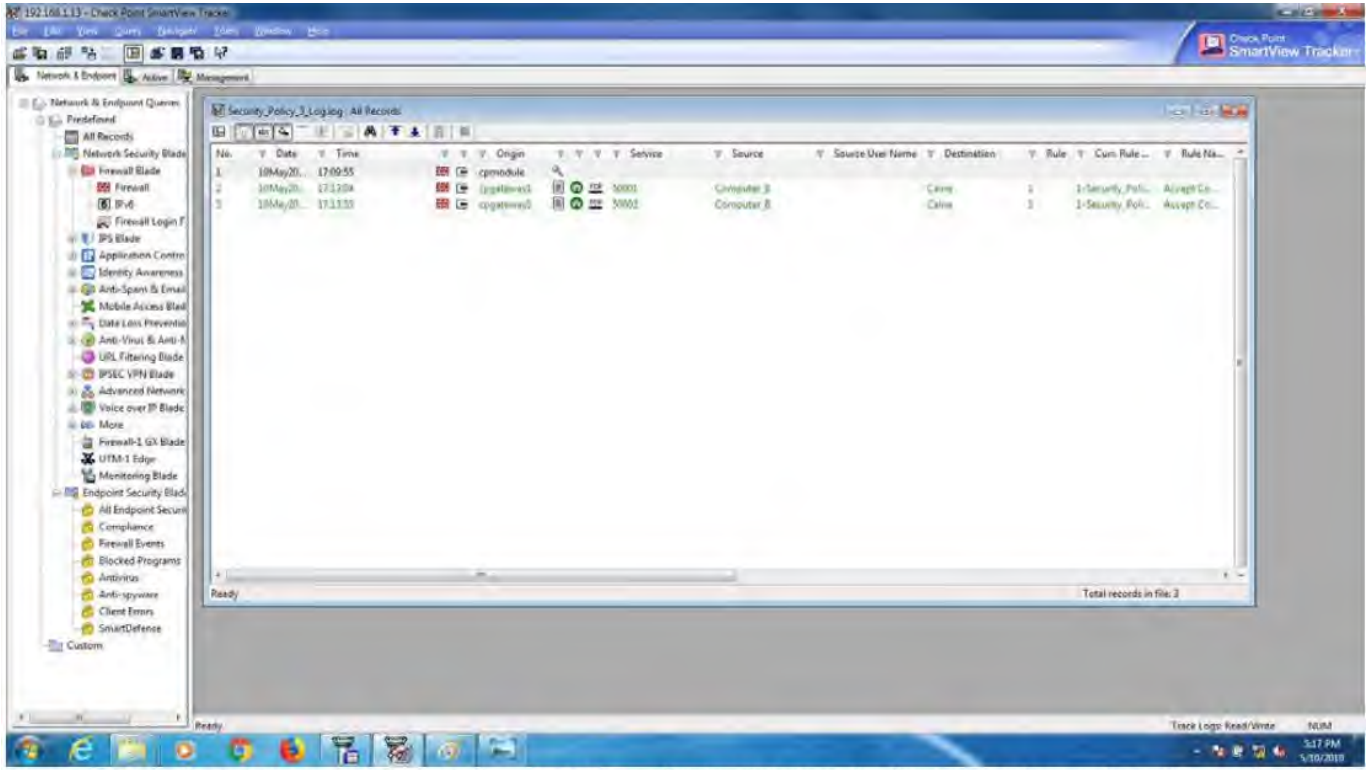
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[h]** 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.	 **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.**

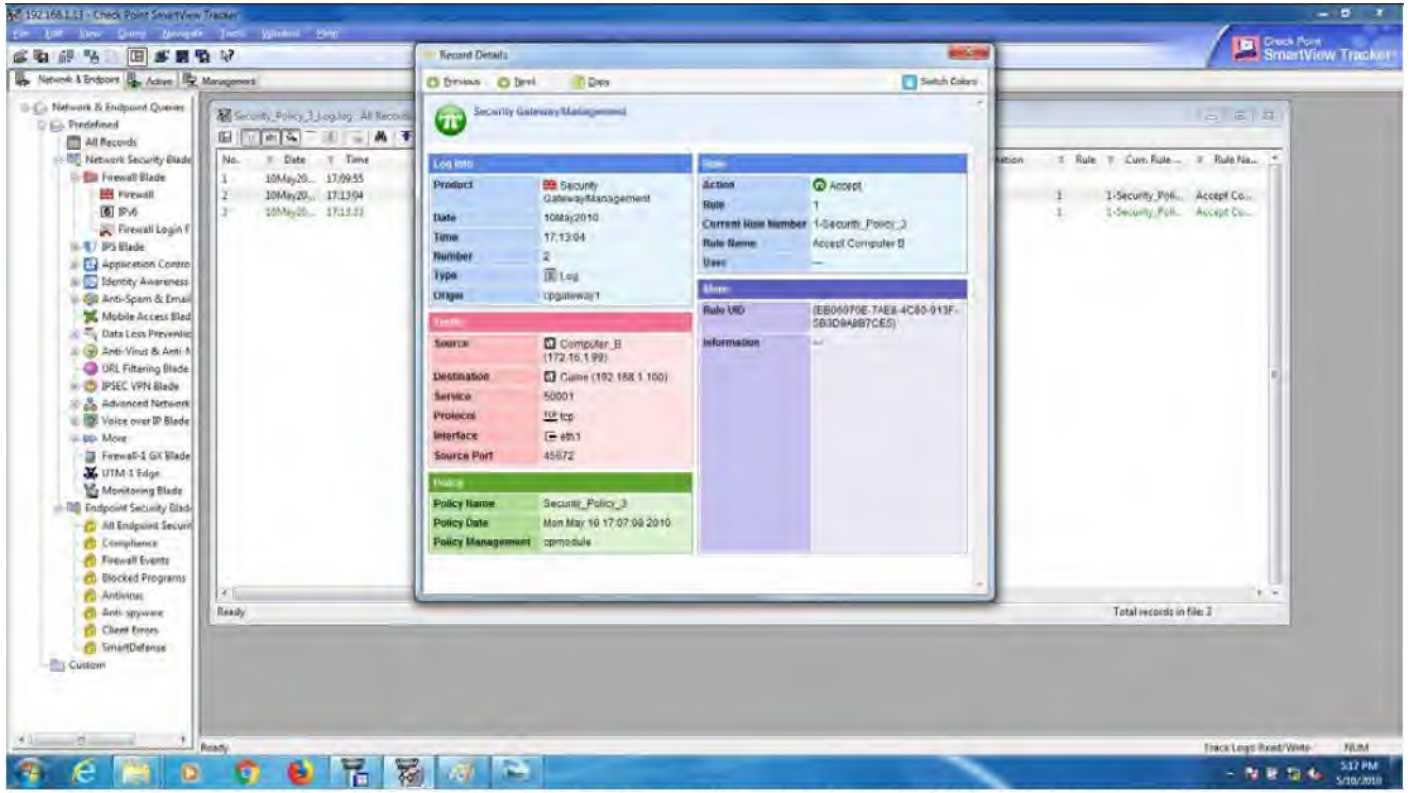
’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[h]** 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.	**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) 17:14:10.851156 172.16.1.99.44628 > 192.168.1.100.50002: . ack 2 win 229 <nop,nop,timestamp 2561757241 64738521> (DF)

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… [h] 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.	 **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.**

’205 Patent Analysis – Check Point R75

’205 Patent:	Check Point R75
17… **[h]** 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.	 **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.**

’205 Patent, Claims 17 and 33 Comparison

17. 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:	33. 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:
receive a plurality of dynamic security policies from the security policy management server,	receive a plurality of dynamic security policies from the security policy management server;
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;	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;
receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;
receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;
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;	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;
receive packets associated with a network protected by the packet security gateway; and	receive packets associated with a network protected by the packet security gateway; 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.	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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 191

Check Point R75 Invalidates the ’205 Patent, Claim 33

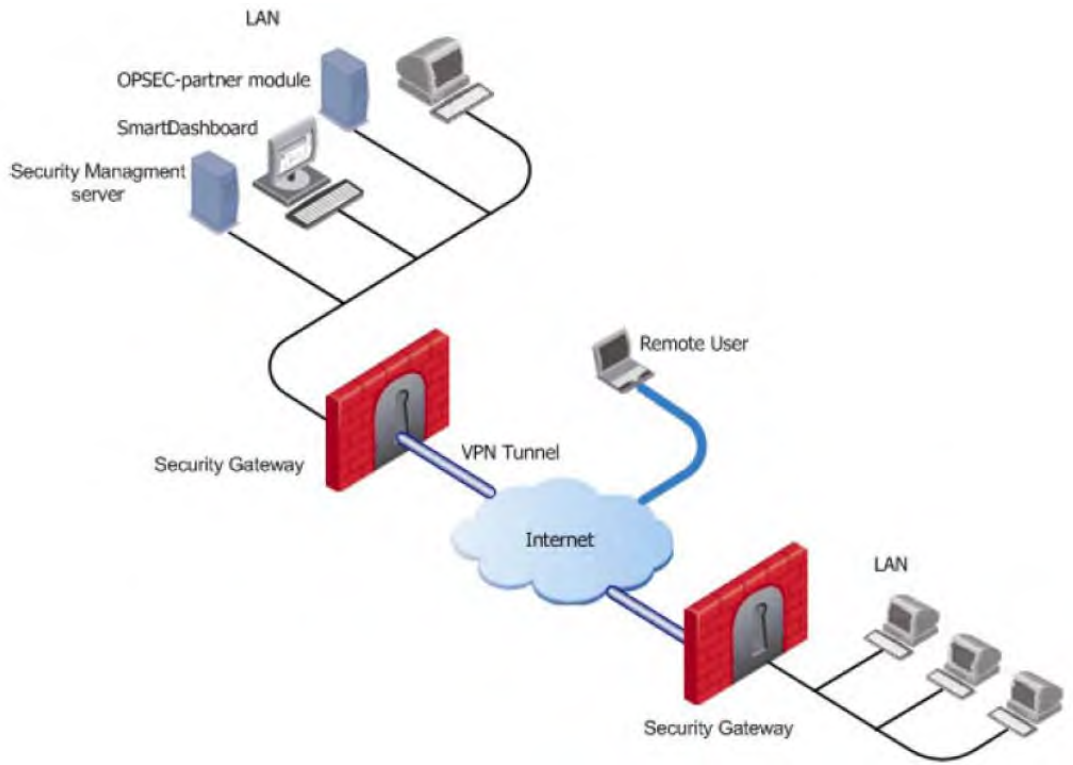
’205 Patent:	Check Point R75
33. [a] One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	✓

Check Point R75 Invalidates the ’213 Patent Claim 1

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. **[a]** 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;	
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – Check Point R75

’722 Patent:	Check Point R75:
1. **[a]** 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;	 **Figure 1: Illustration of a typical deployment consisting of two security gateways and a security management server (configurable using the “SmartDashboard” GUI).[3]**

’213 Patent Analysis – Check Point R75

’722 Patent:	Check Point R75:
1. **[a]** 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;	 Figure 129. Screenshot of Check Point SmartDashboard GUI showing dynamic security policy with an explicit firewall rule to allow packets.

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. **[a]** 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;	
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – Check Point R75

’722 Patent:	Check Point R75:
1. **[b]** receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	 Figure 138. Screenshot showing properties of the HTTP request header to be sent from Computer B to Computer A.

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. **[a]** 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;	
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – Check Point R75

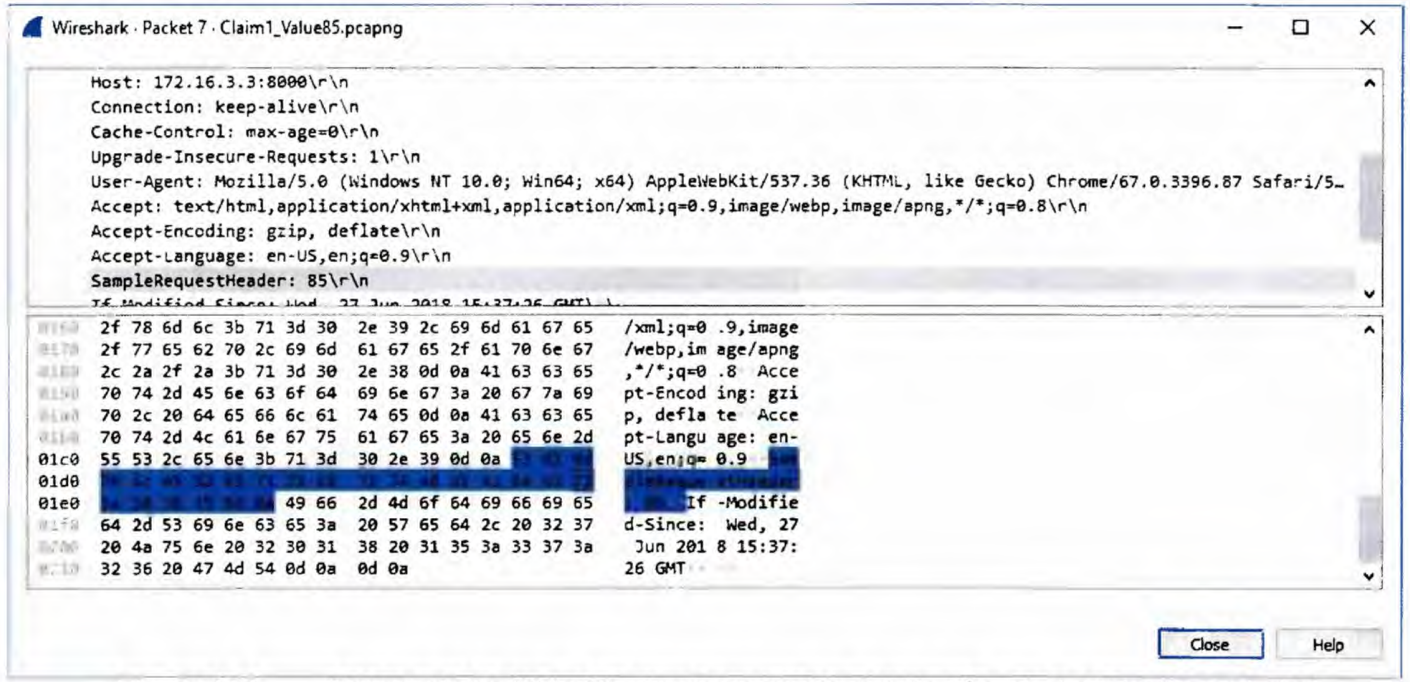
’722 Patent:	Check Point R75:
1. [c] identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information;	

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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 200

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. **[a]** 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;	
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – Check Point R75

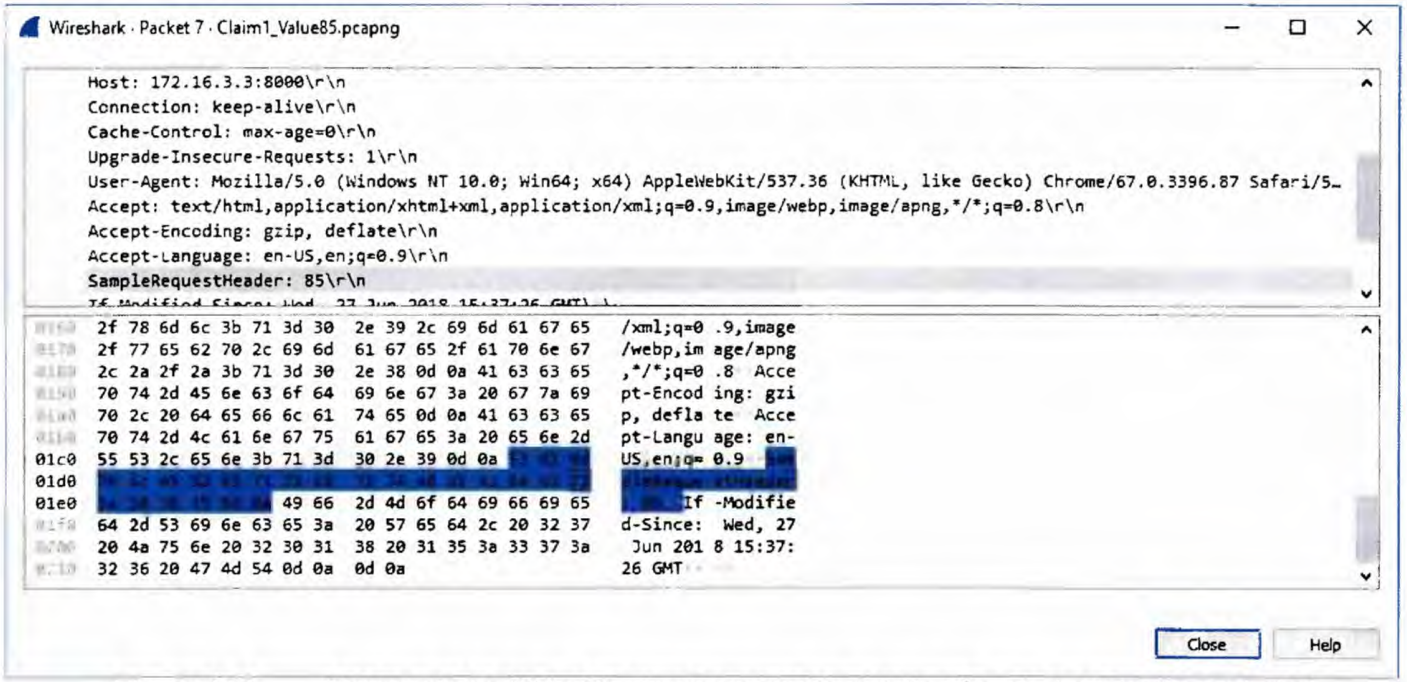
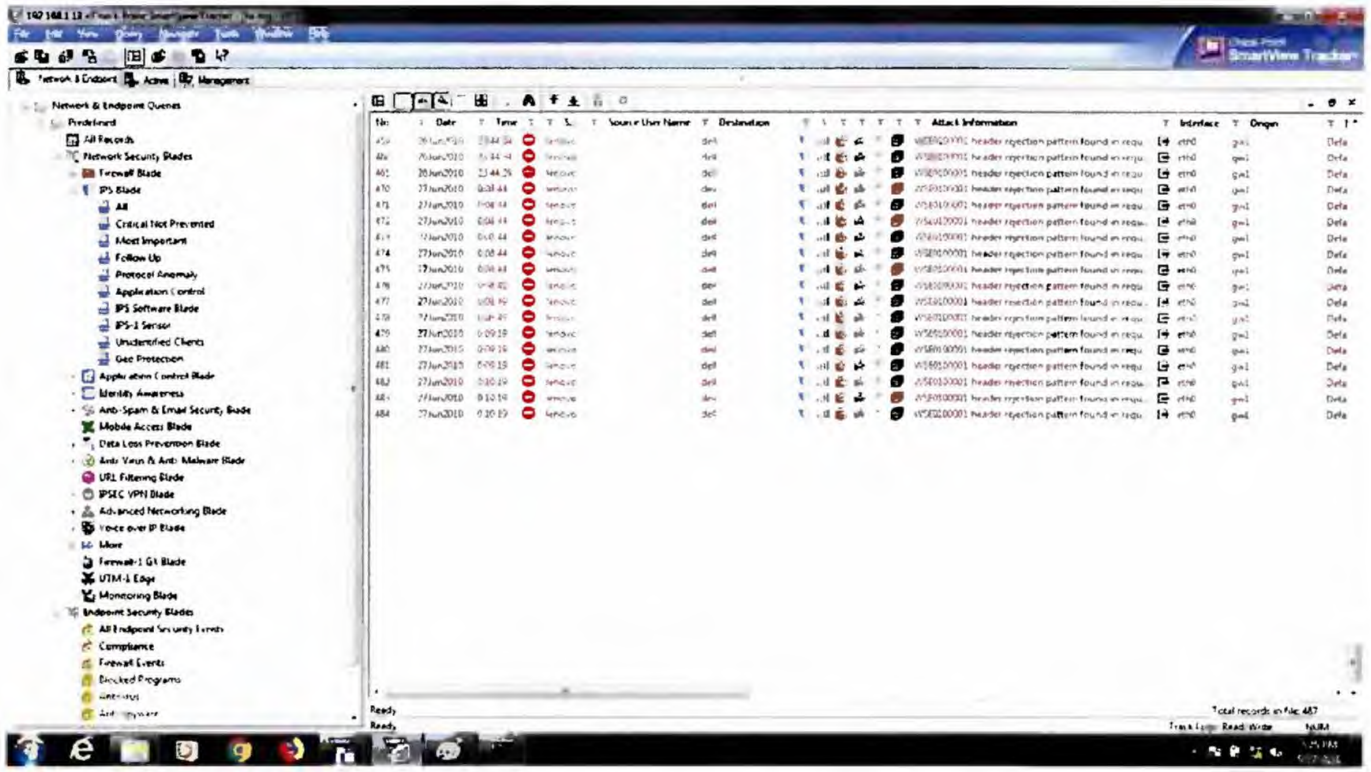
’722 Patent:	Check Point R75:
1. [d] performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises	

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.

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. **[a]** 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – Check Point R75

’722 Patent:	Check Point R75:
1. [e] 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;	 Figure 145. Screenshot of Check Point SmartView Tracker listing packets rejected based on configured dynamic security policies including rejection based on header content.

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. **[a]** 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	✓
[f] 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	
[g] 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	
[h] 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.	

’213 Patent Analysis – Check Point R75

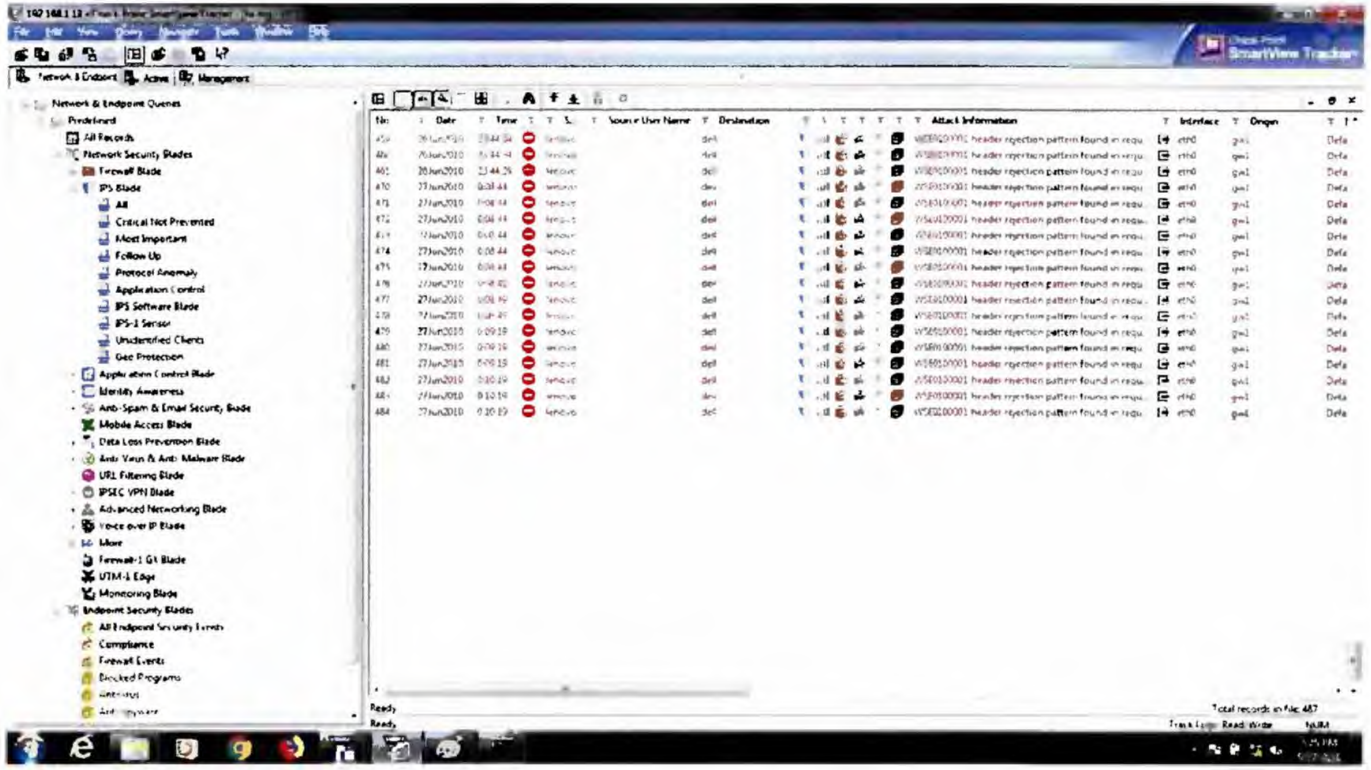
’722 Patent:	Check Point R75:
1. [f] generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and	

Figure 145. Screenshot of Check Point SmartView Tracker listing packets rejected based on configured dynamic security policies including rejection based on header content.

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. [a] 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	✓
[f] 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	✓
[g] 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	
[h] 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.	

’213 Patent Analysis – Check Point R75

’722 Patent:	Check Point R75:
1. [g] 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	

Figure 146. Screenshot showing reformatted packet log information from Check Point R75.

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. **[a]** 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;	✓
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	✓
[c] 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;	✓
[d] 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	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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.	

’213 Patent Analysis – Check Point R75

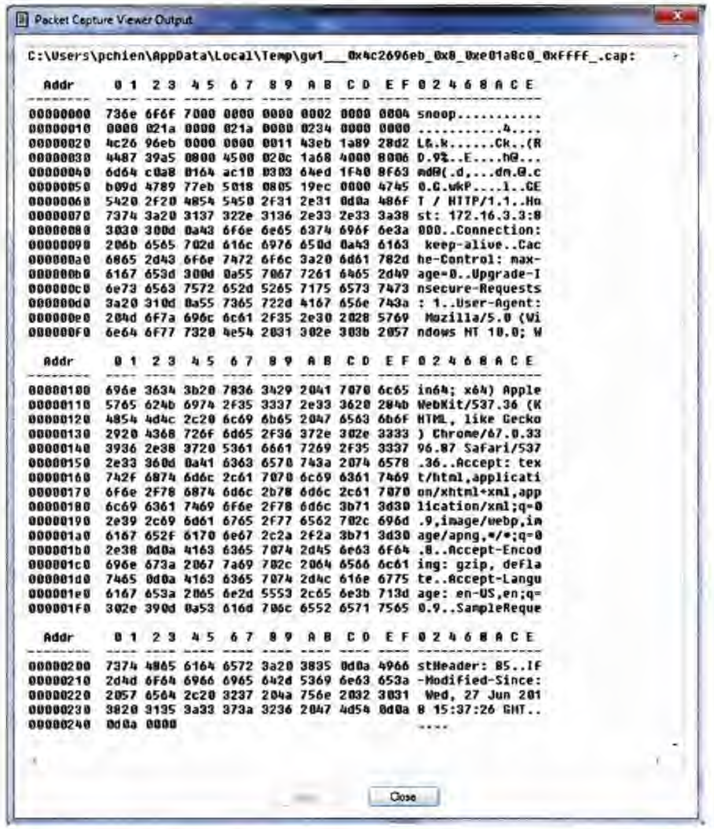
’722 Patent:	Check Point R75:
1. [h] routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.	

Figure 147. Screenshot of the Packet Capture View Output from Check Point R75

Check Point R75 Invalidates the ’213 Patent, Claim 1

’213 Patent:	Check Point R75
1. [a] 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;	
[b] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;	
[c] 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;	
[d] 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	
[e] 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;	
[f] 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	
[g] 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	
[h] 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.	

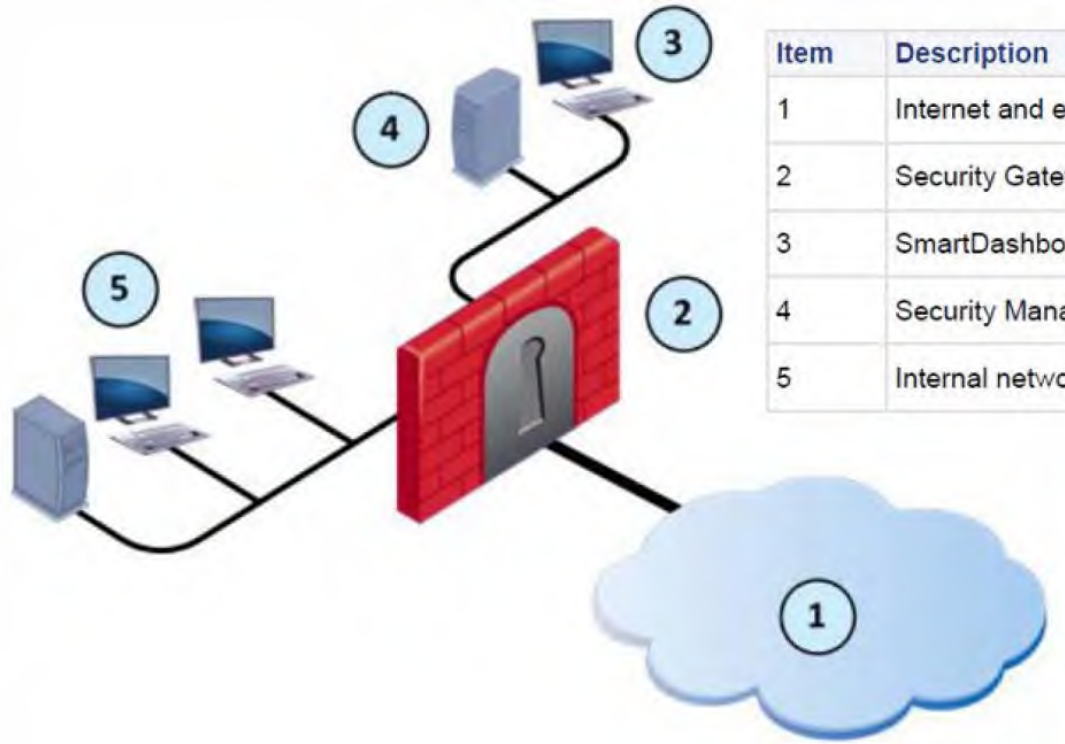

Check Point R77

Check Point R77 Invalidates the ’722 Patent Claim 1

Check Point R77 Invalidates the ’722 Patent, Claim 1

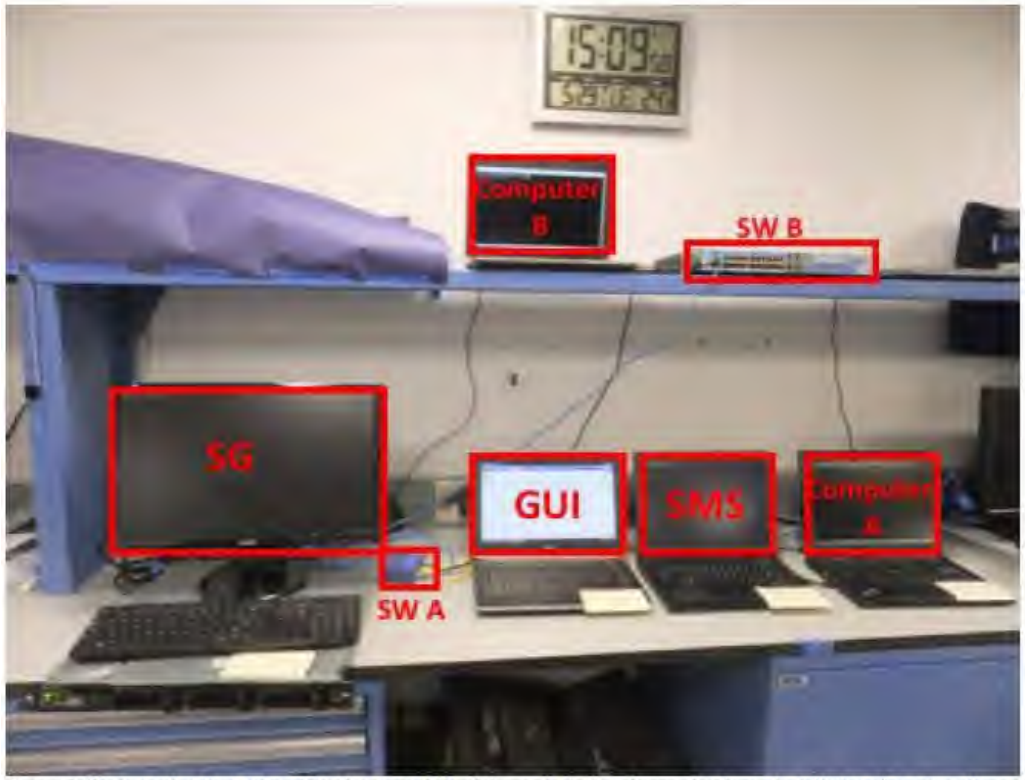
’722 Patent:	Check Point R77
1. **[a]** A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;	
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – Check Point R77

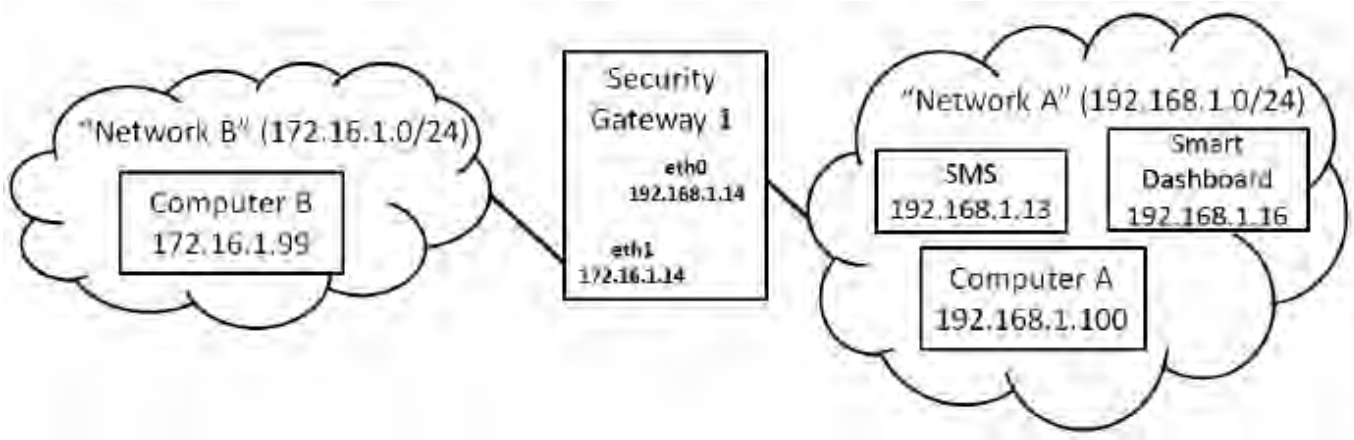
’722 Patent:	Check Point R77
1. **[a]** A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;	 Figure 1: Typical deployment of a security gateway and a security management server (configurable using the SmartDashboard graphical user interface, or GUI). [3]

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

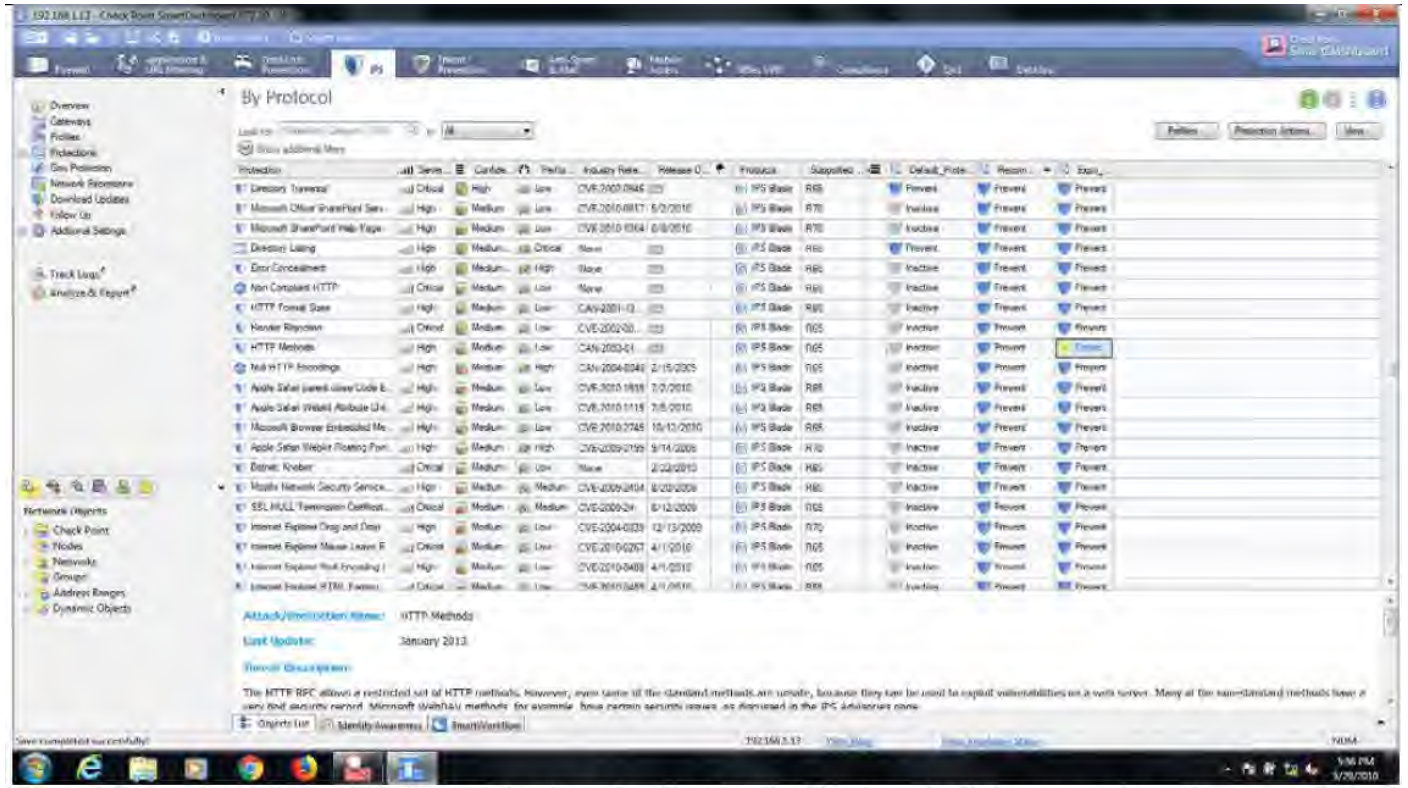
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1. **[a]** 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;	 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.

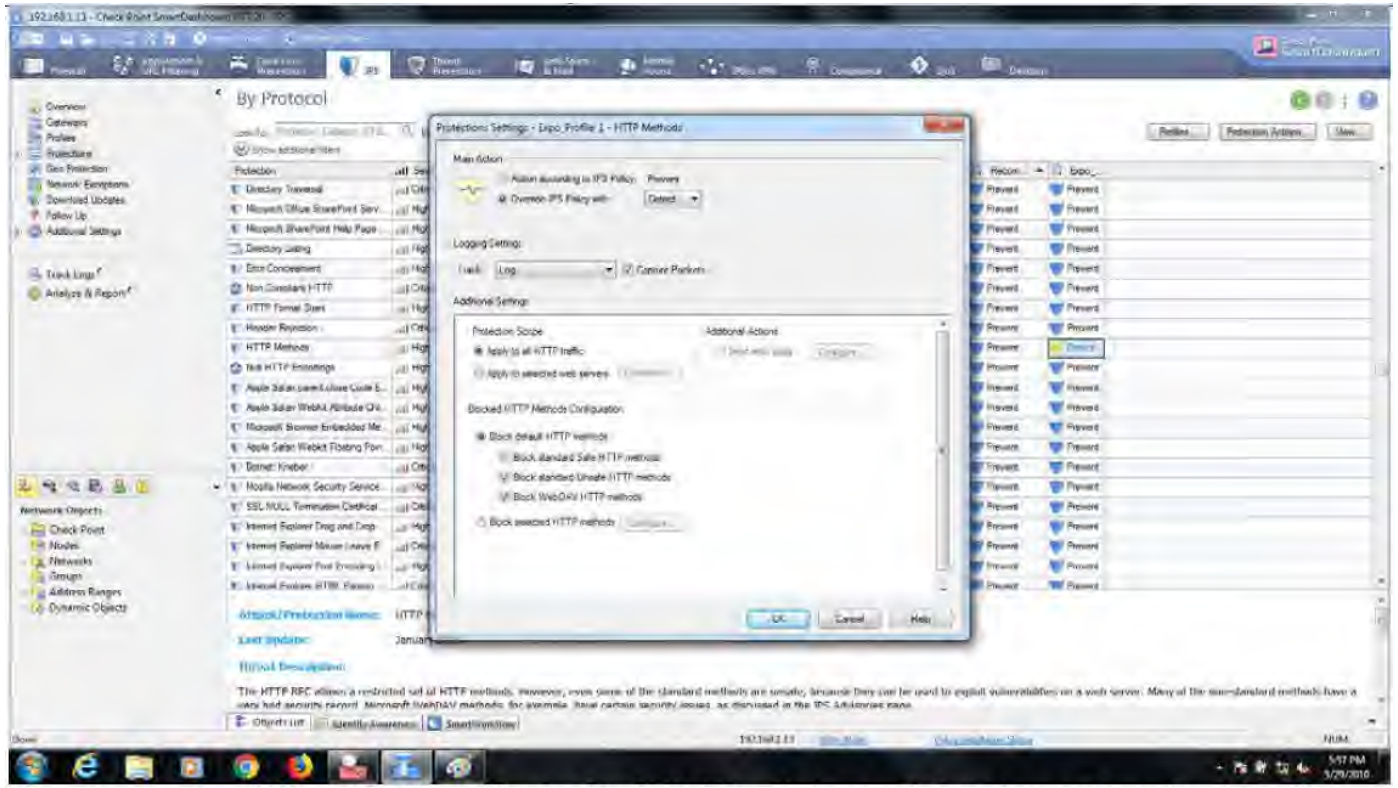
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1. **[a]** 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;	 **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.**

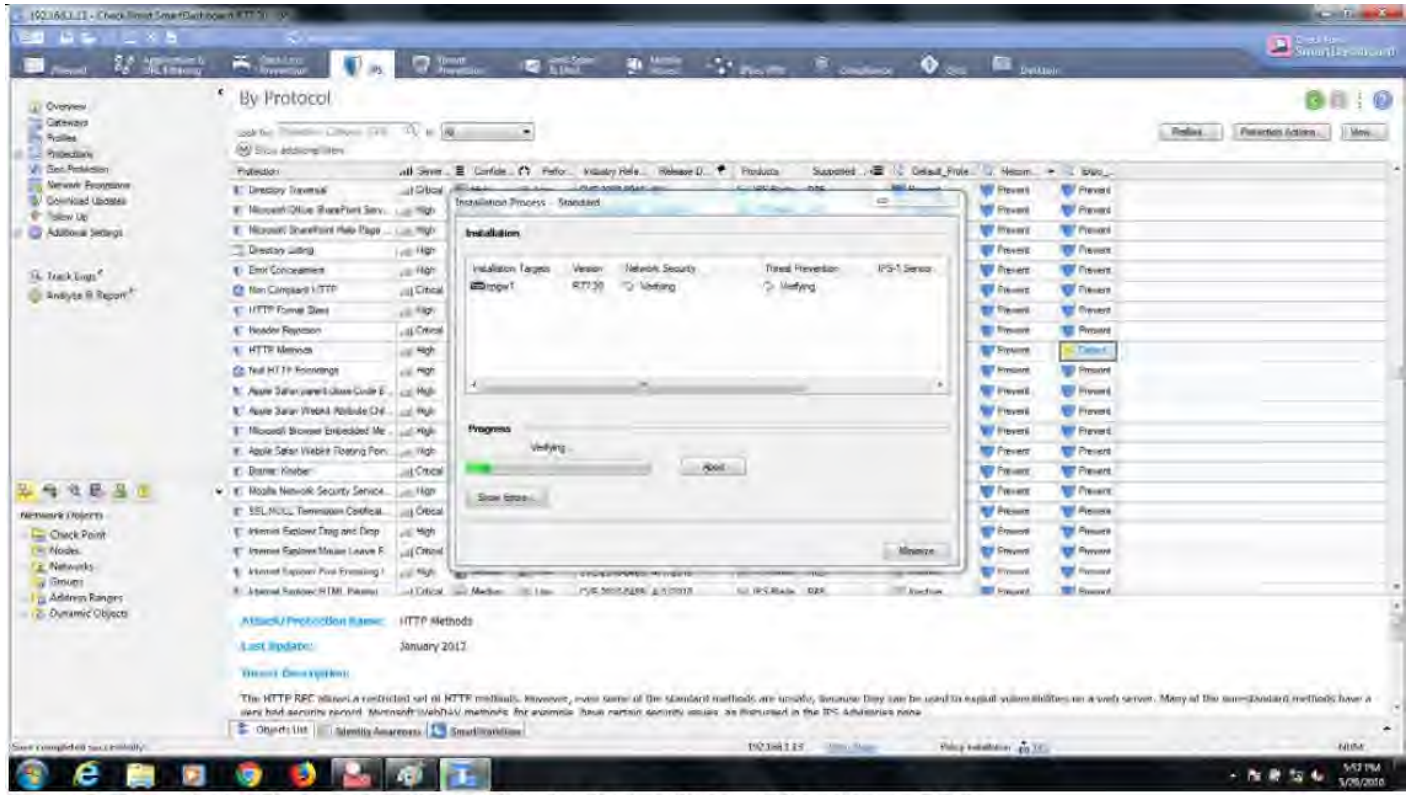
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1. **[a]** 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;	 **Figure 4: Screenshot of the SmartDashboard showing a plurality of packet-filtering rules that correspond to various network threats.**

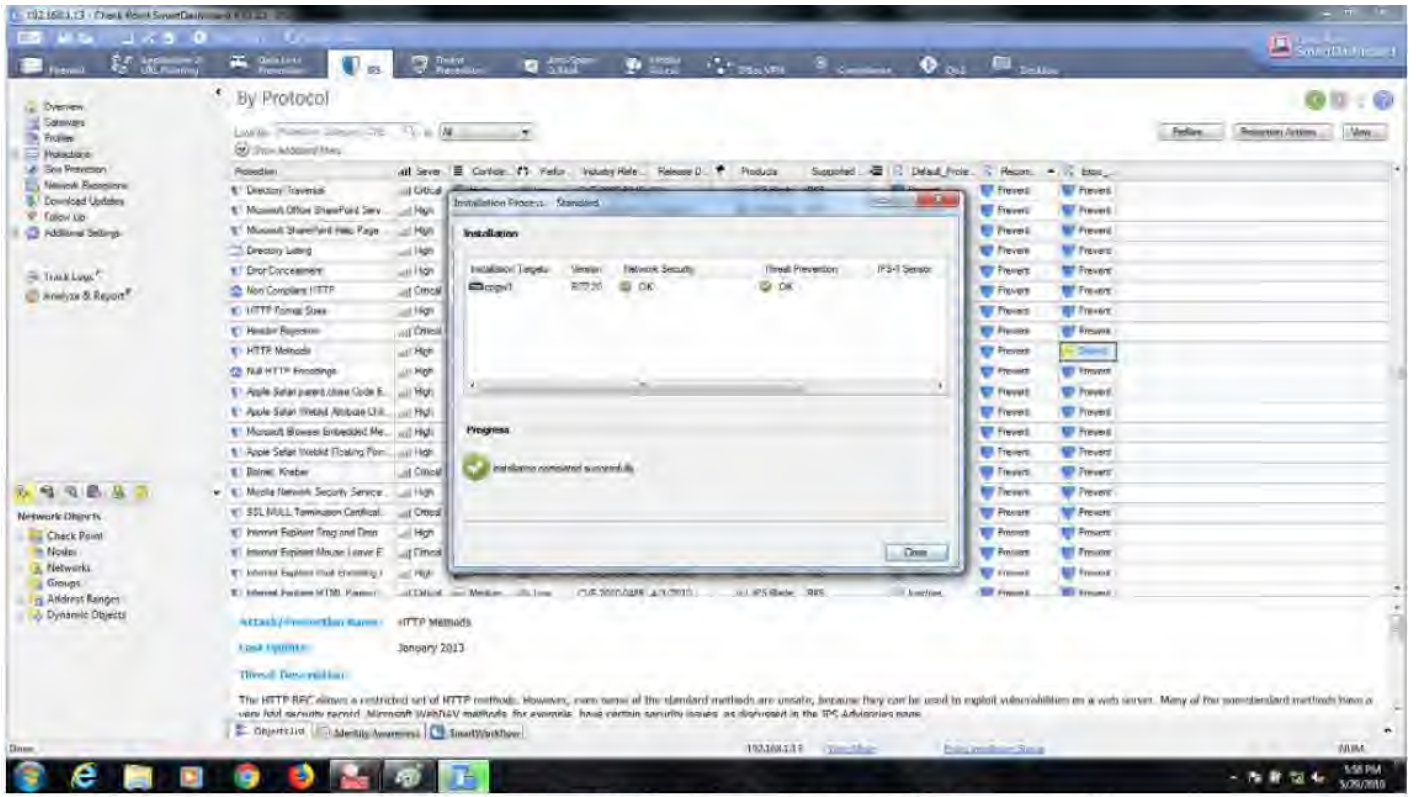
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1. **[a]** 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;	 **Figure 5: Screenshot of the SmartDashboard showing that the HTTP methods network threat is set to “Detect” mode for this policy.**

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1. **[a]** 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;	 Figure 6: Screenshot of the SmartDashboard showing the installation of the policy on SG 1.

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1. **[a]** 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;	 **Figure 7: Screenshot of the SmartDashboard showing that the policy installation on SG 1 was successful.**

Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. **[a]** 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – Check Point R77

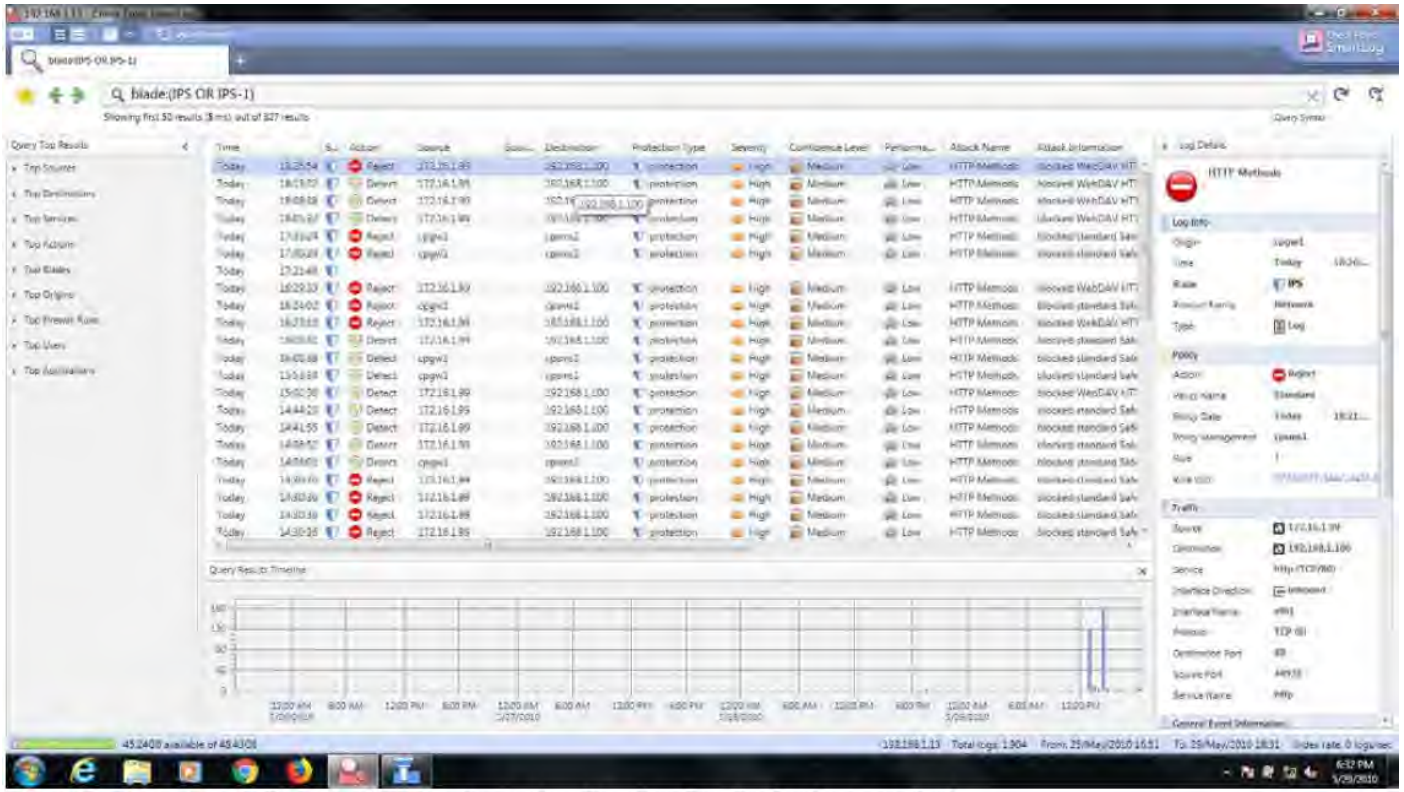
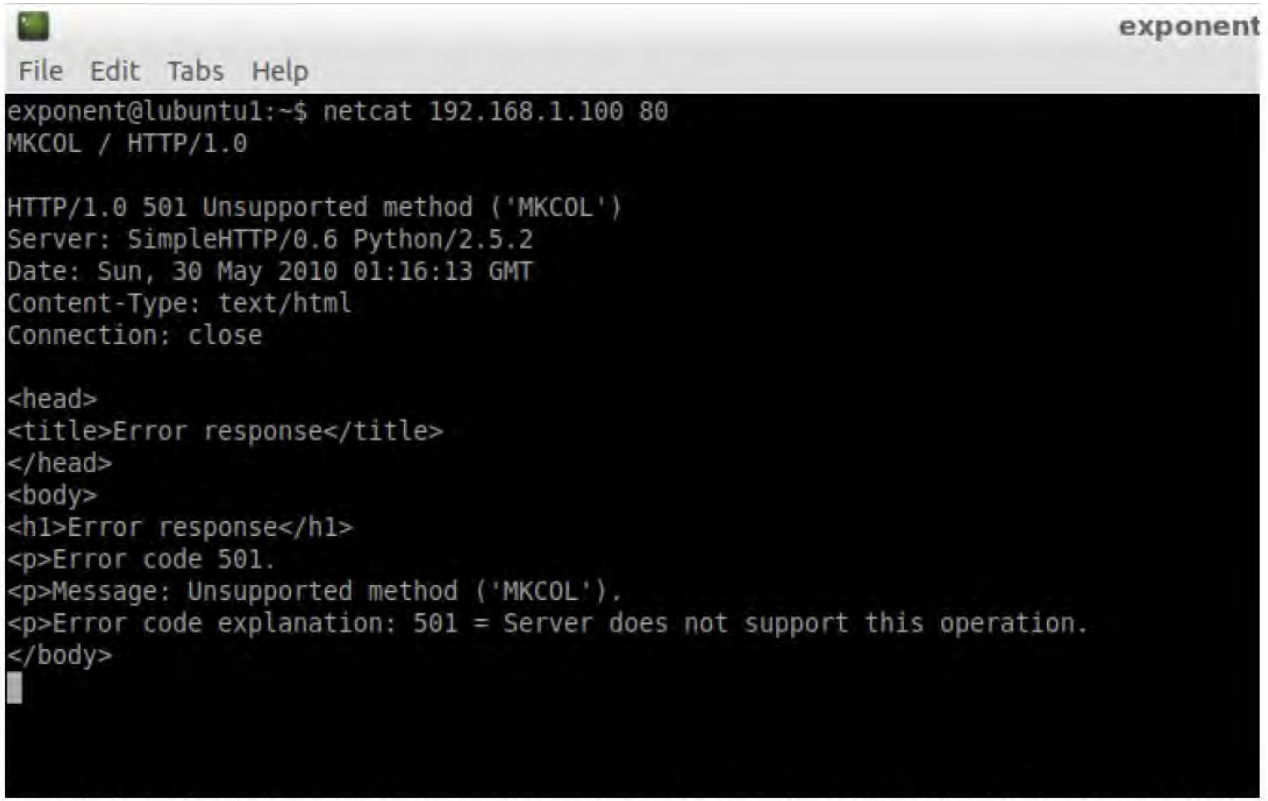
’722 Patent:	Check Point R77
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	

Figure 8: Screenshot of the SmartLog showing a plurality of packets having been received.

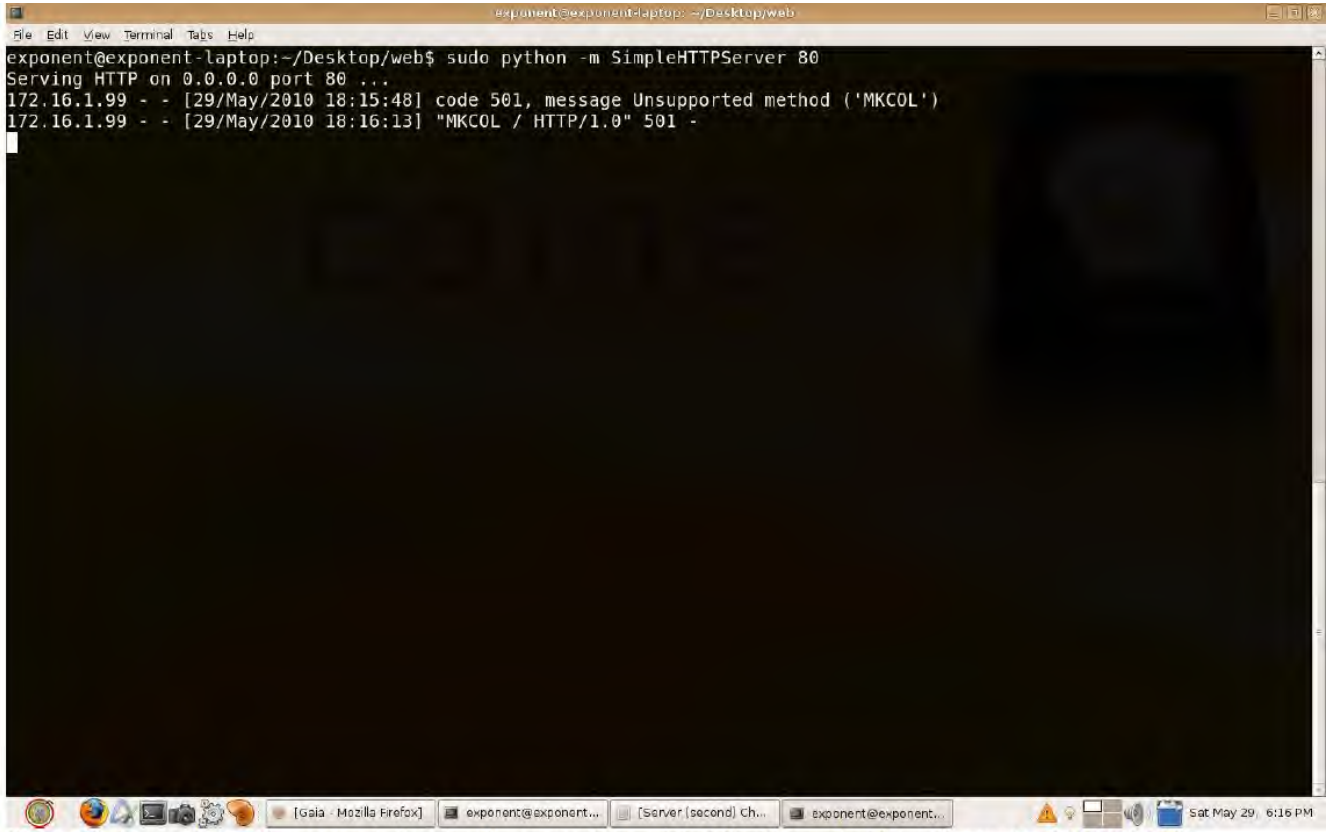
Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. **[a]** 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… [c] 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;	 **Figure 9: Screenshot of Computer B illustrating the connection to Computer A (192.168.1.100) and successful send of the first packet.**

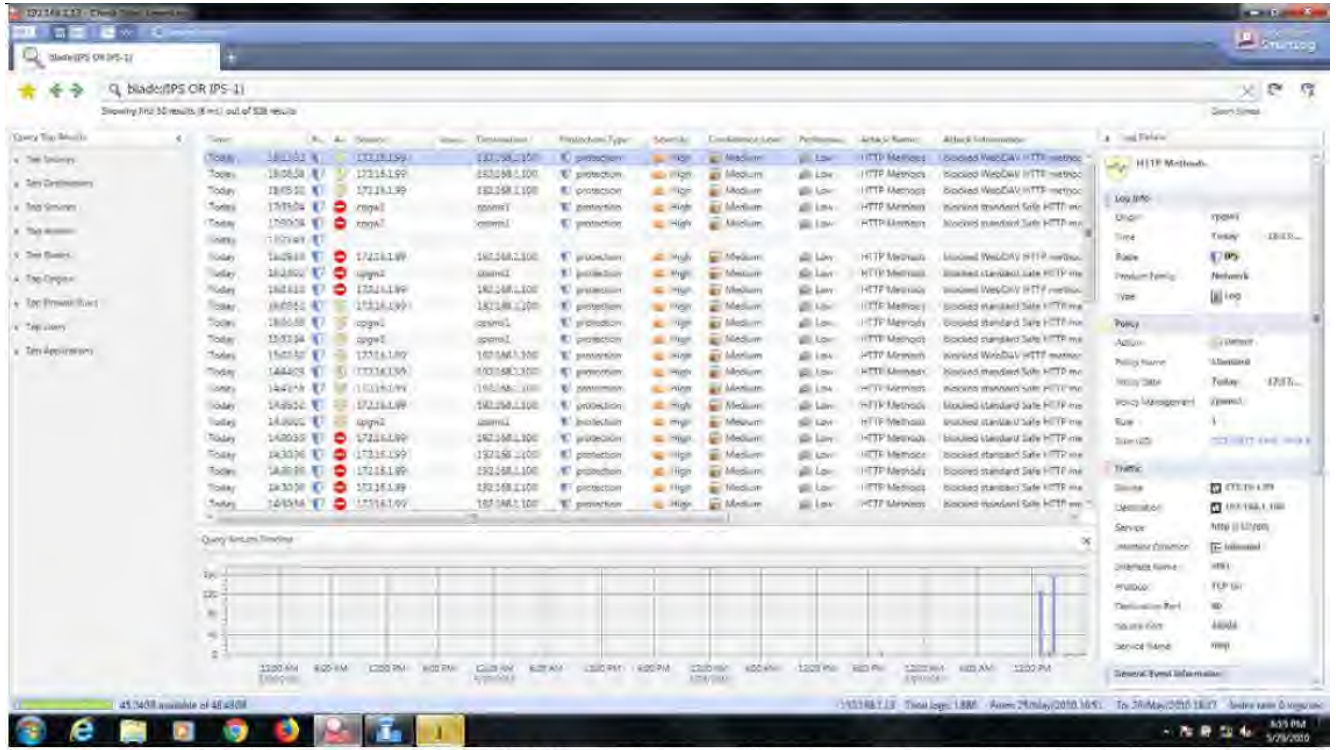
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… [c] 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;	 Figure 10: Screenshot of Computer A showing the successful receipt of the first packet from Computer B (172.16.1.99).

Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. **[a]** 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[d]** 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;	 **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).**

Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. **[a]** 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – Check Point R77

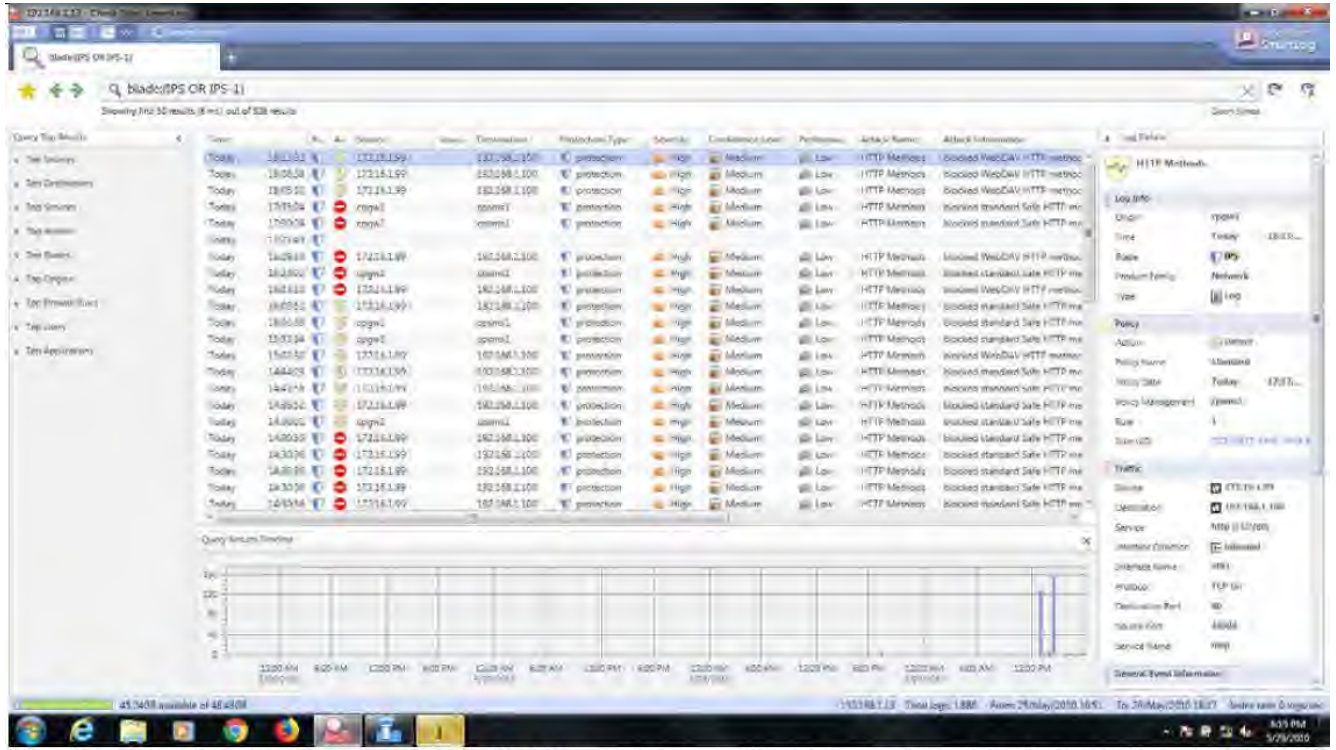
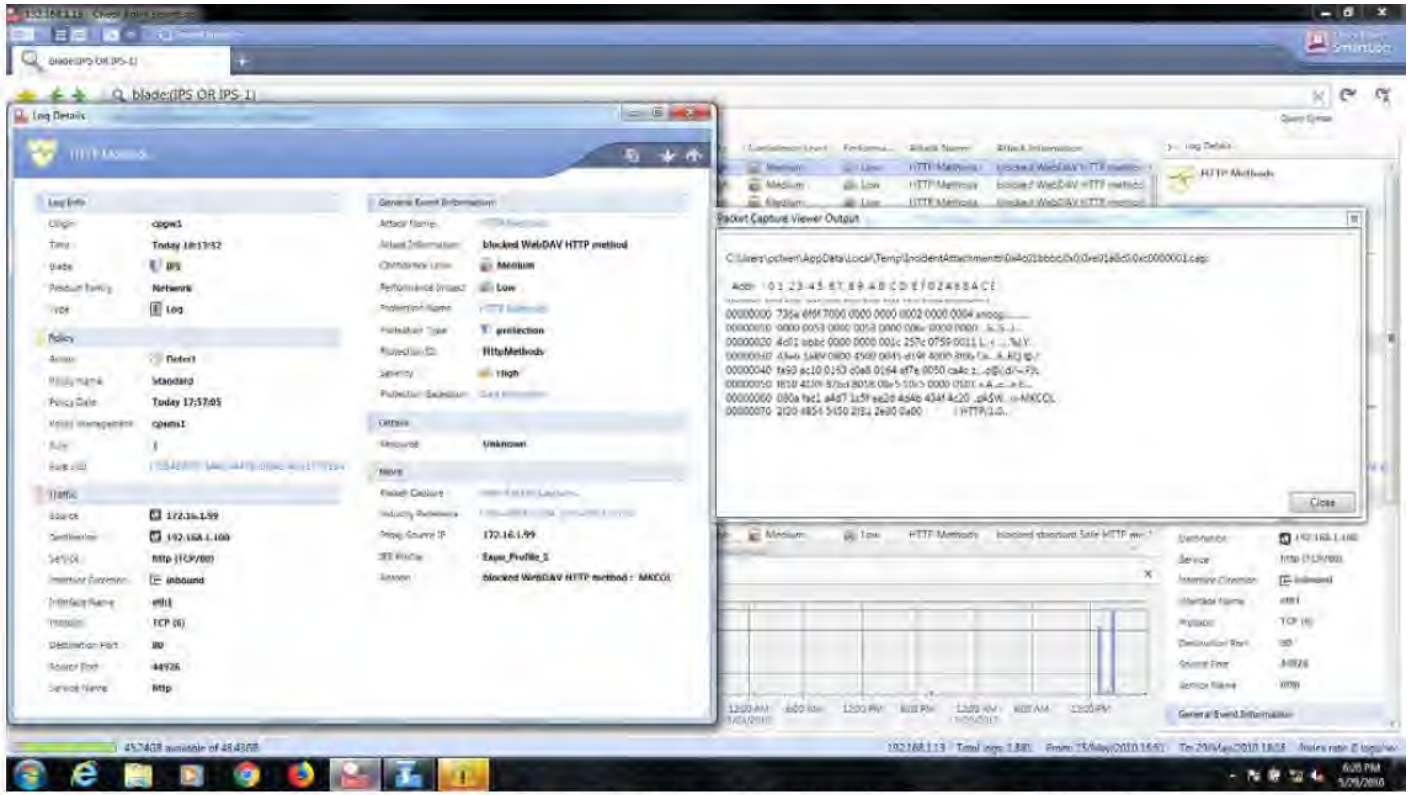
’722 Patent:	Check Point R77
1… **[e]** causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;	

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).

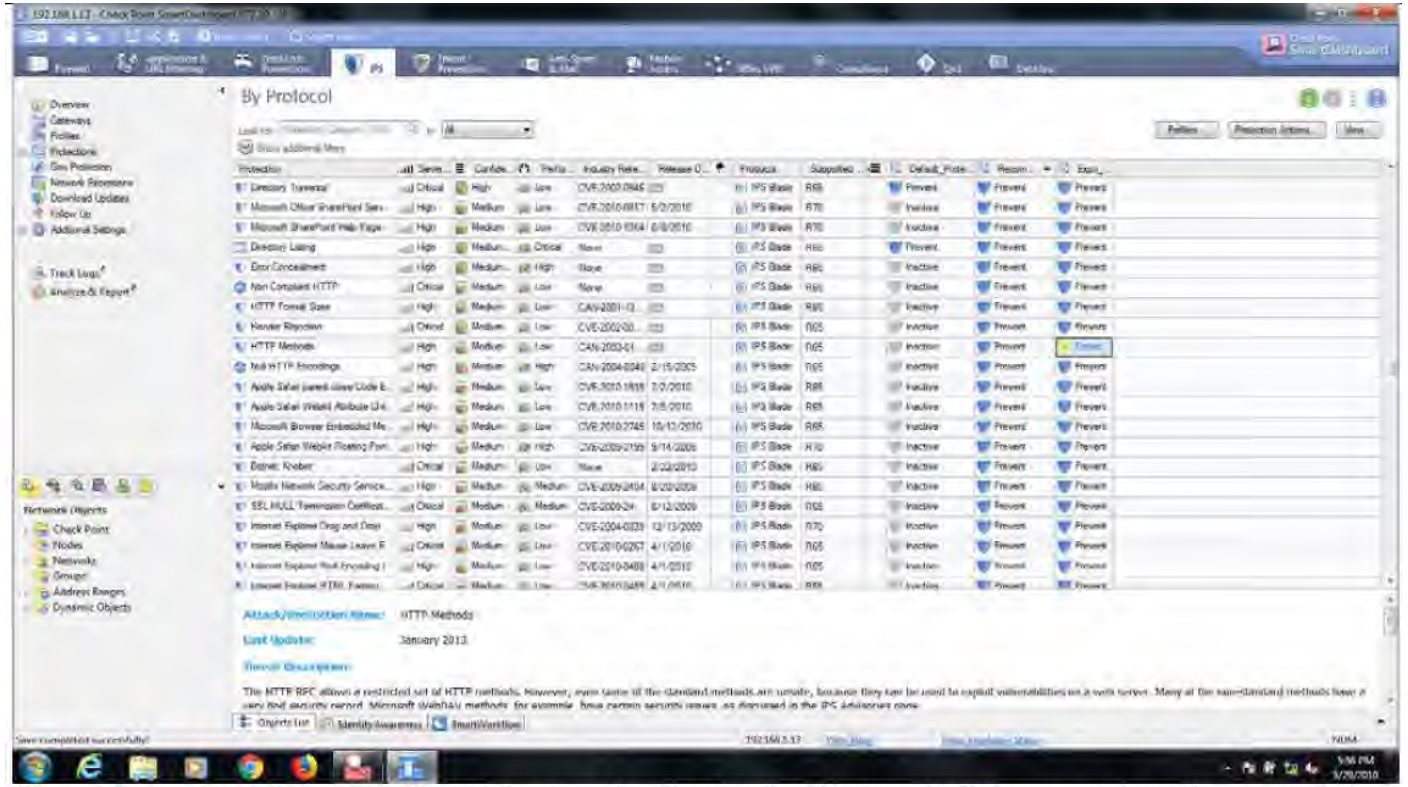
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[e]** 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;	 Figure 12: Screenshot of the SmartLog showing the details of the packets allowed to move toward the destination.

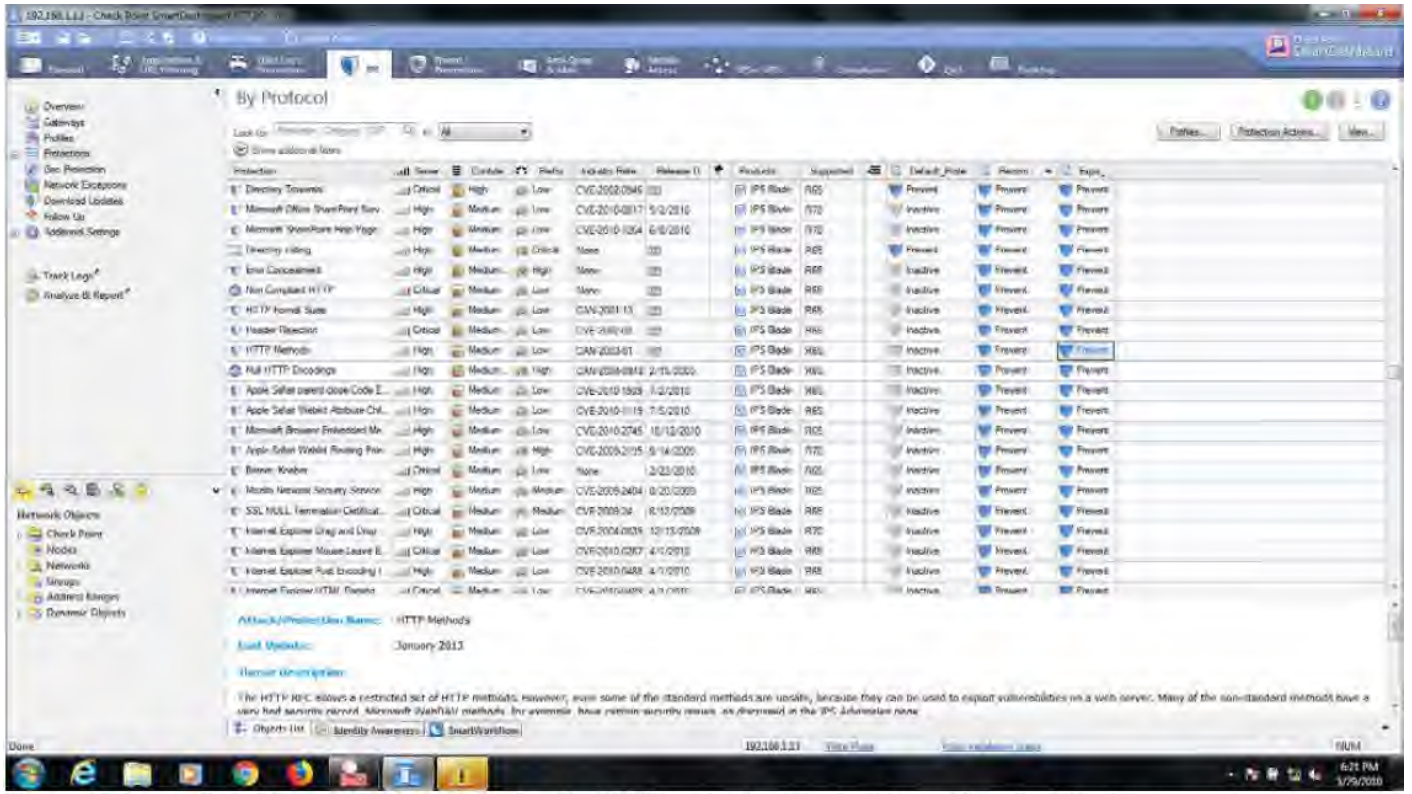
Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. **[a]** 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

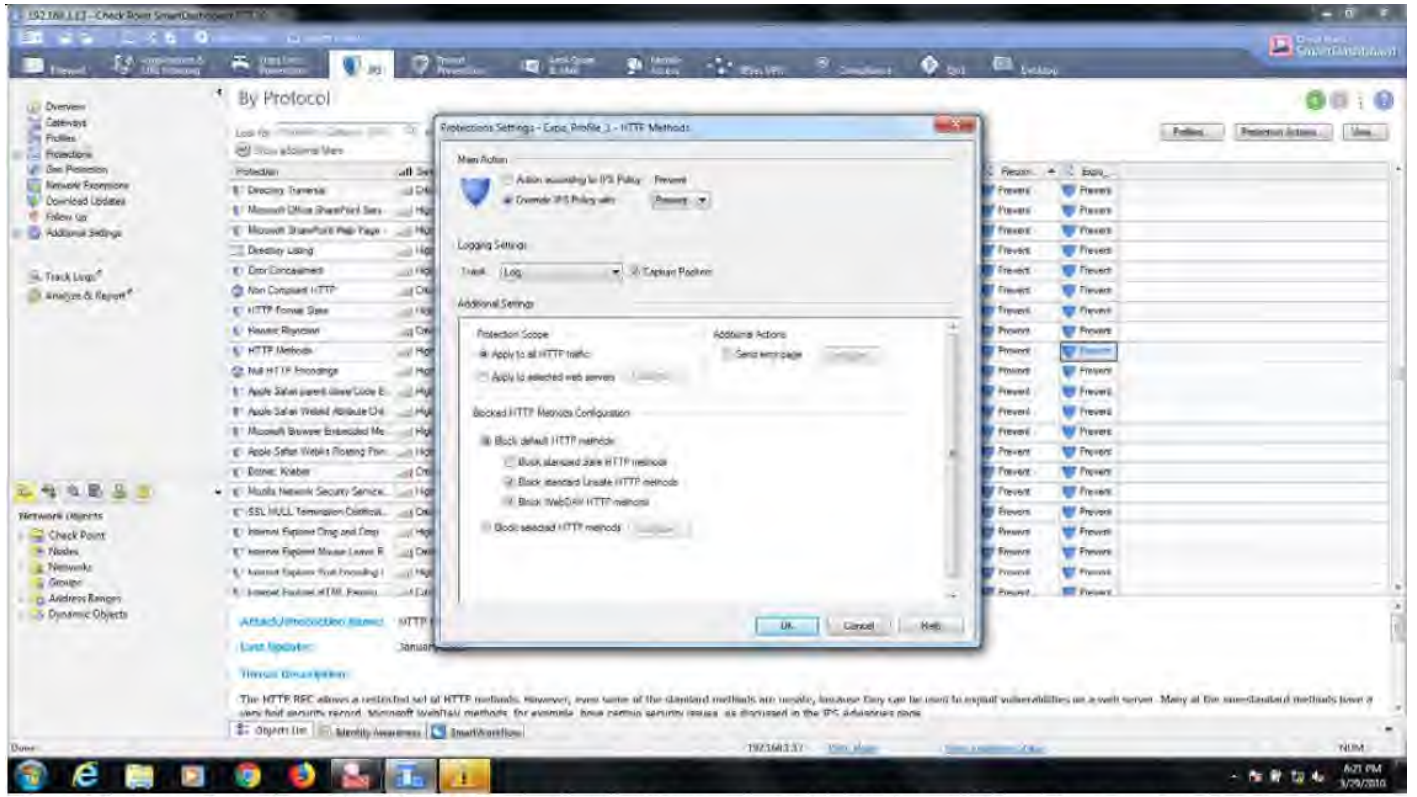
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[f]** 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	 **Figure 4: Screenshot of the SmartDashboard showing a plurality of packet-filtering rules that correspond to various network threats.**

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… [f] 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	 Figure 13: Screenshot of SmartDashboard showing the HTTP methods policy in “Prevent” mode. This change was in response to user action.

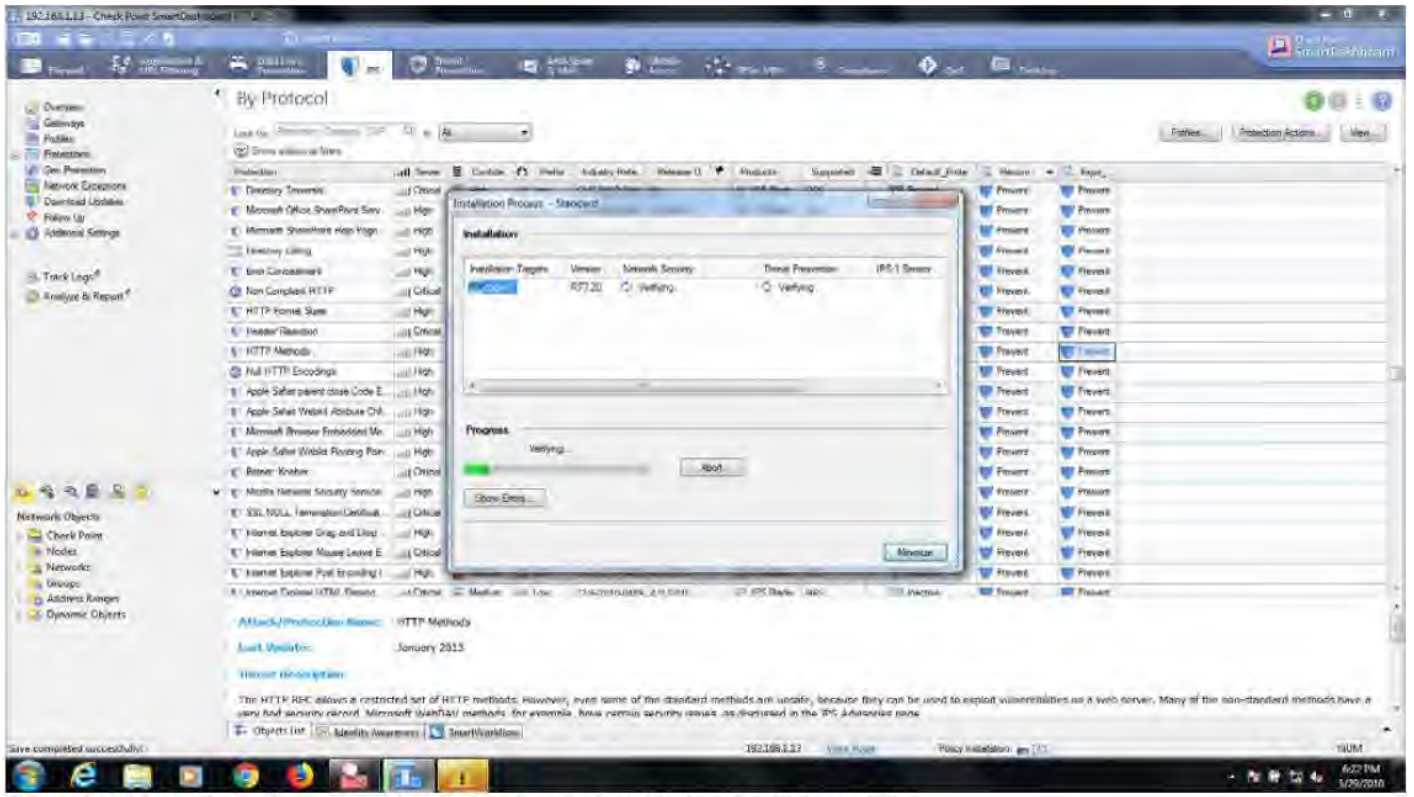
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[f]** 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	 **Figure 14: Screenshot of SmartDashboard showing detailed information of the HTTP methods policy after changing the policy to “Prevent.”**

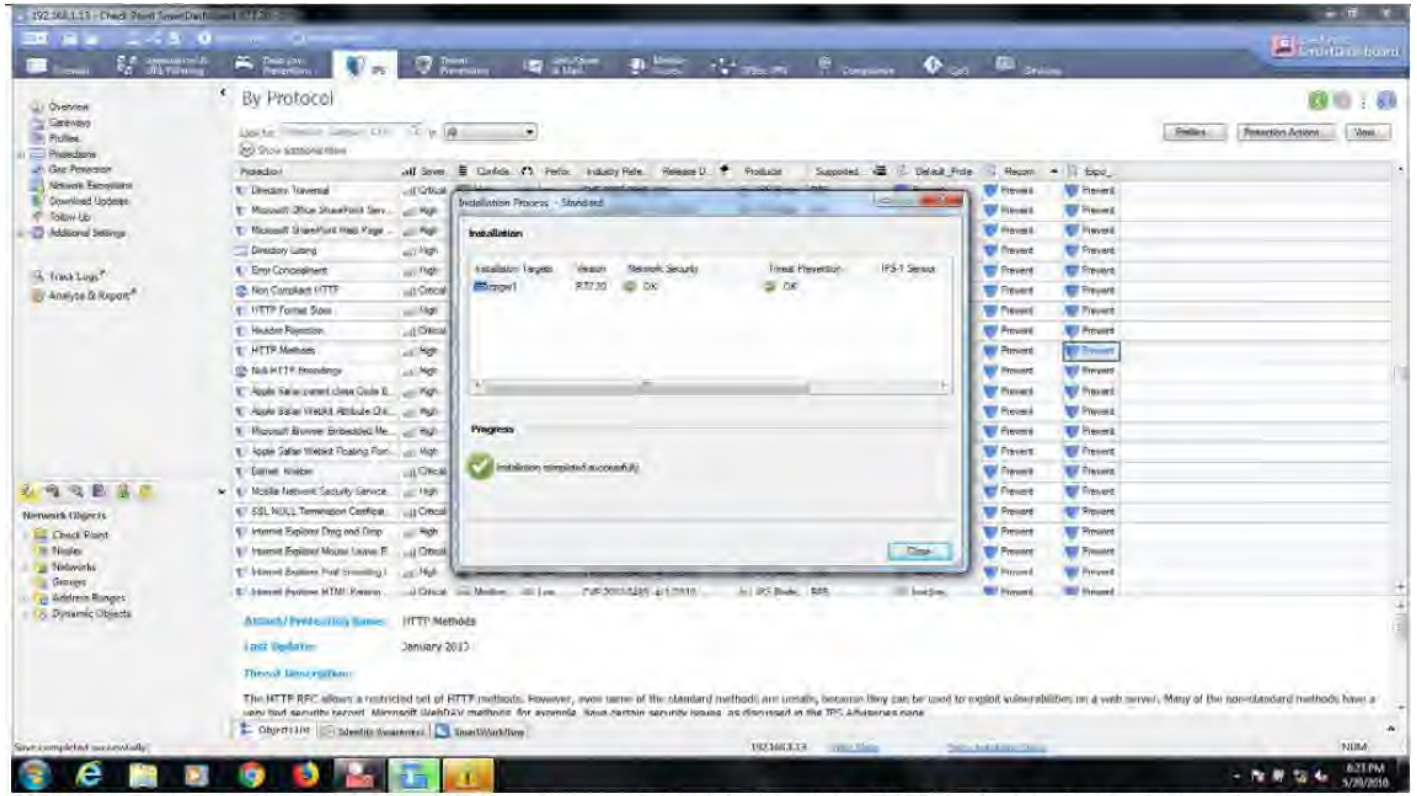
Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… [g] 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	 Figure 15: Screenshot of SmartDashboard showing the installation of policies on SG 1.

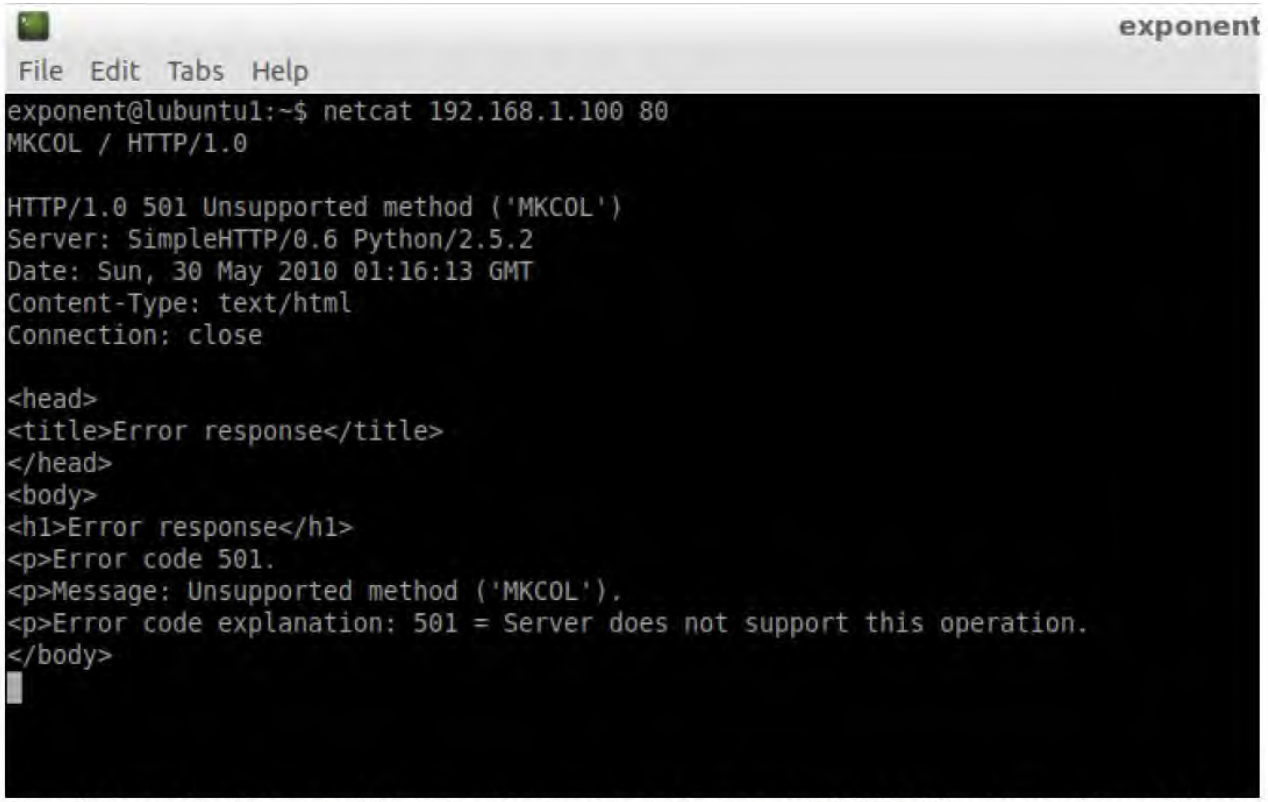
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… [g] 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	 Figure 16: Screenshot of SmartDashboard showing successful installation of the HTTP methods policy in “Prevent” mode on SG 1.

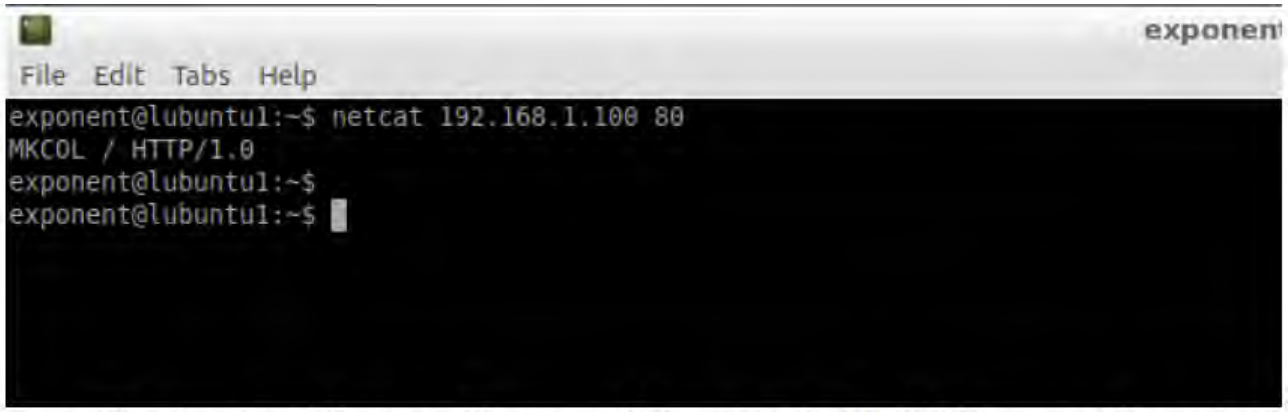
Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

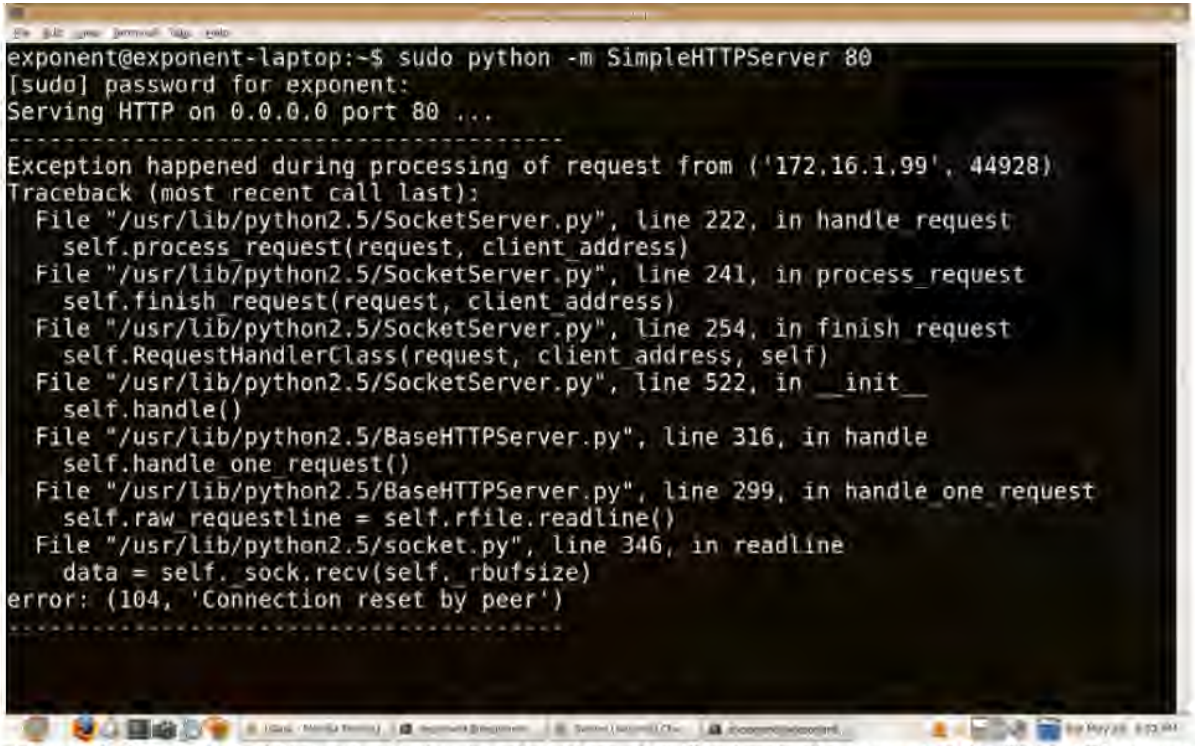
’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[h]** 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	 **Figure 9: Screenshot of Computer B illustrating the connection to Computer A (192.168.1.100) and successful send of the first packet.**

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[h]** 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	 **Figure 17: Screenshot of Computer B unsuccessfully sending the WebDAV request to Computer A.**

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[h]** 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	 **Figure 18: Screenshot of Computer A showing that the packet-filtering device prevented the WebDAV request from Computer B.**

Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – Check Point R77

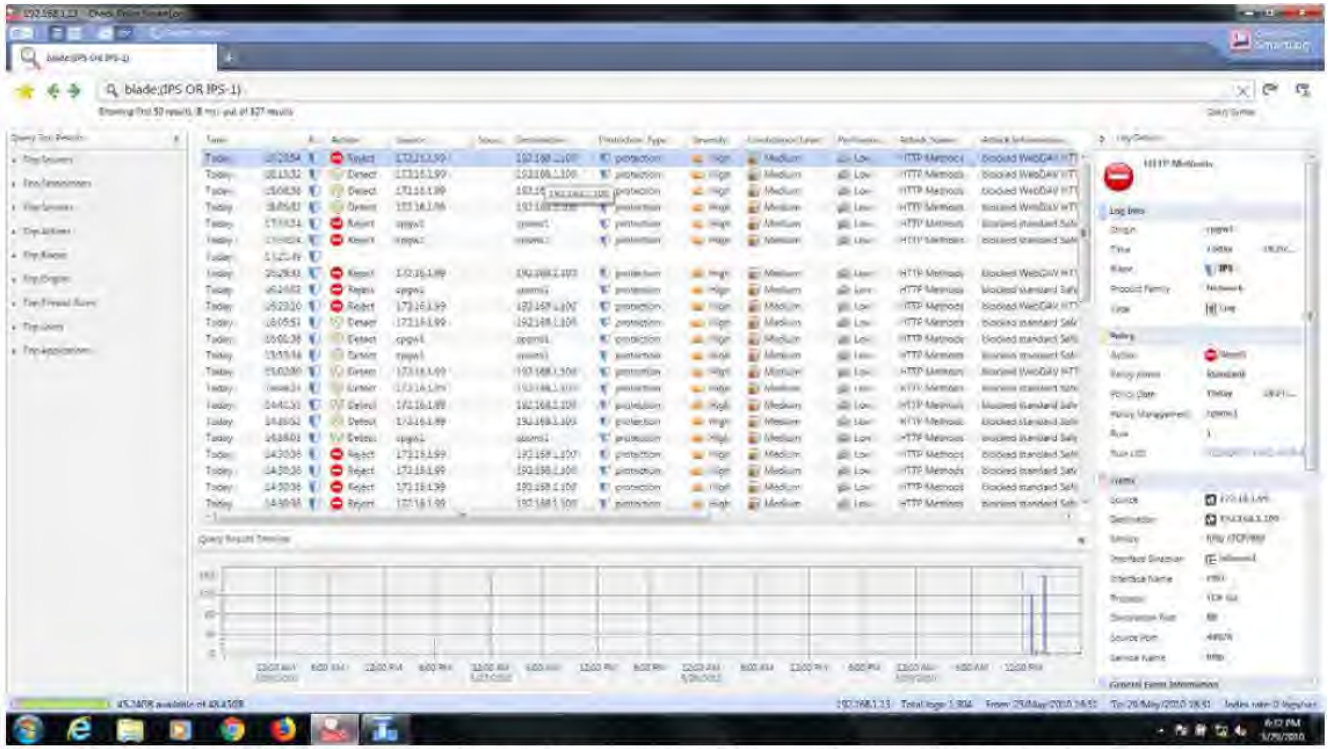
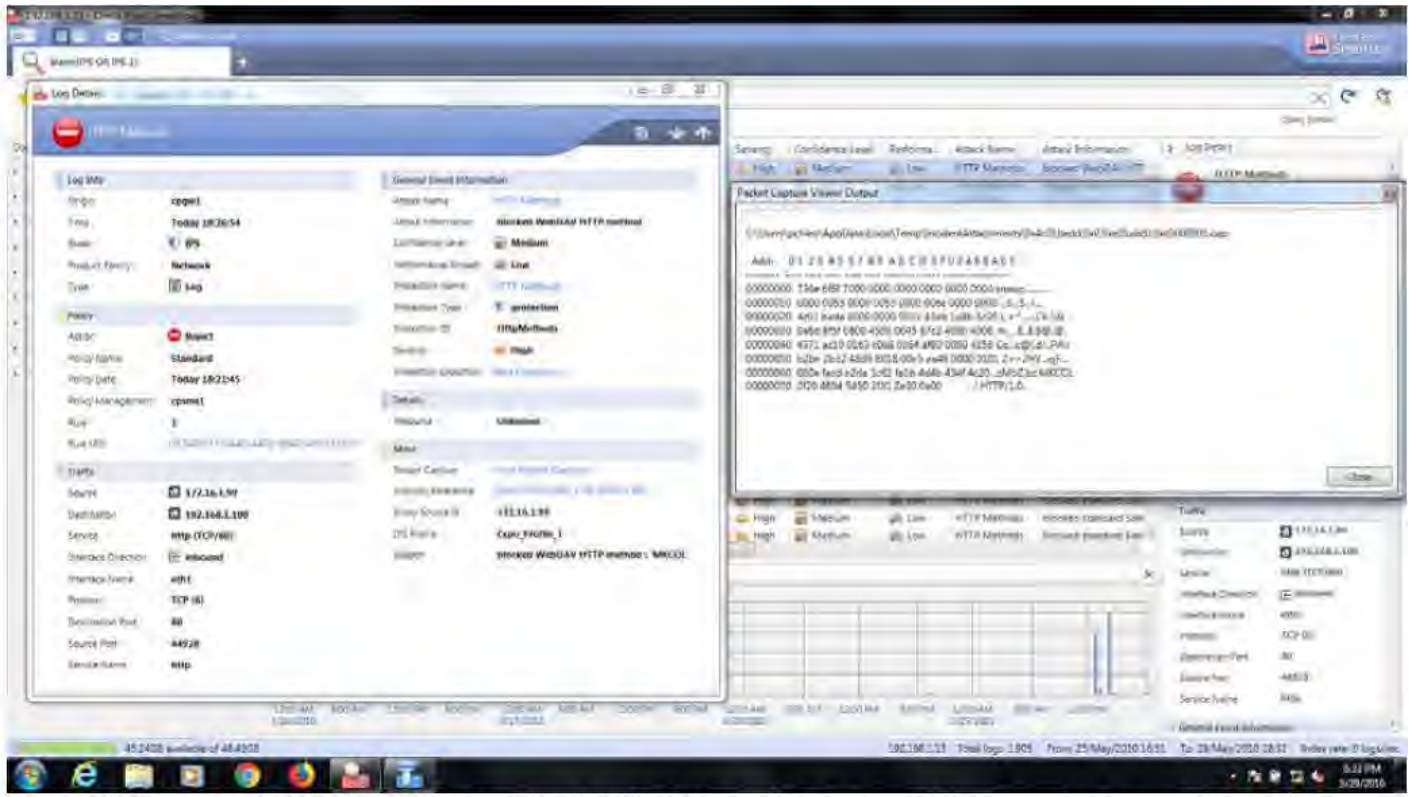
’722 Patent:	Check Point R77
1… **[i]** communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	

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).

Check Point R77 Invalidates the ’722 Patent, Claim 1

’722 Patent:	Check Point R77
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	✓
[j] 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.	

’722 Patent Analysis – Check Point R77

’722 Patent:	Check Point R77
1… **[j]** 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.	 Figure 20: Screenshot of the SmartLog showing details of the packets prevented from moving toward the destination.

Check Point R77 Invalidates the ’722 Patent, Claim 1

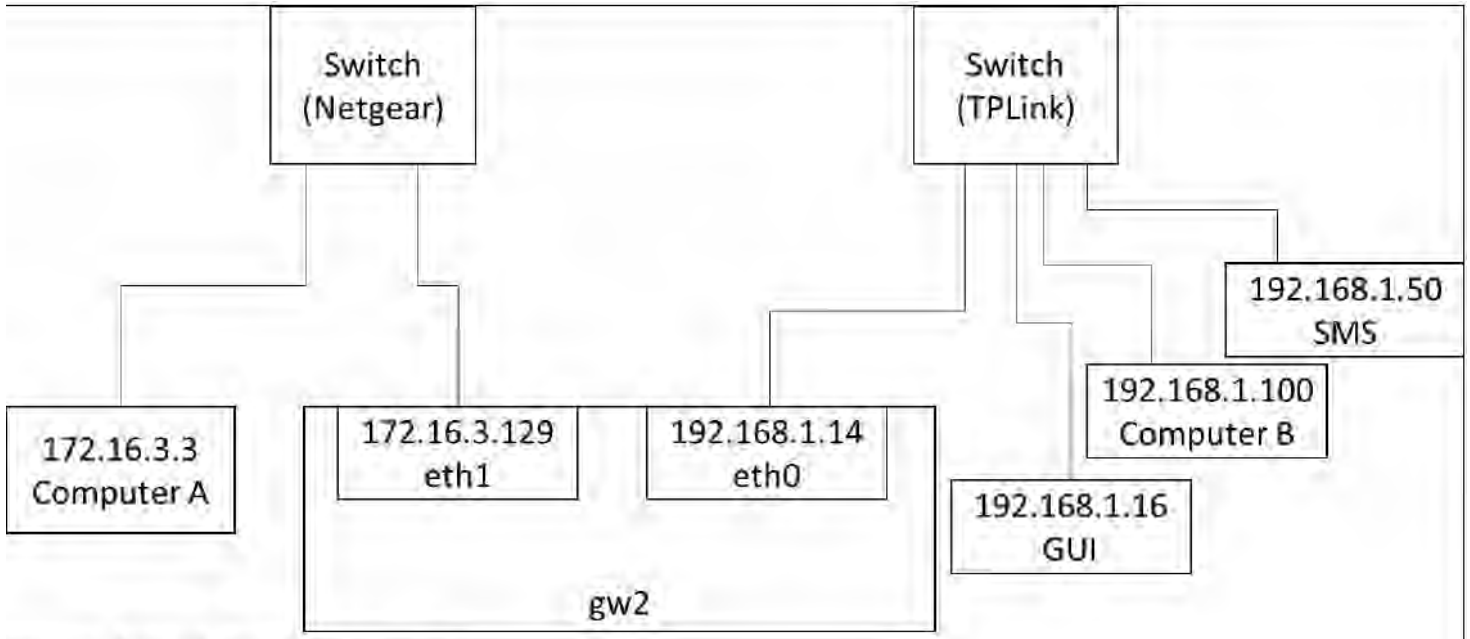
’722 Patent:	Check Point R77
1. [a] A method comprising: receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	✓
[j] 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.	✓

Check Point R77 Invalidates the ’856 Patent Claim 24

Check Point R77 Invalidates the ’856 Patent, Claim 24

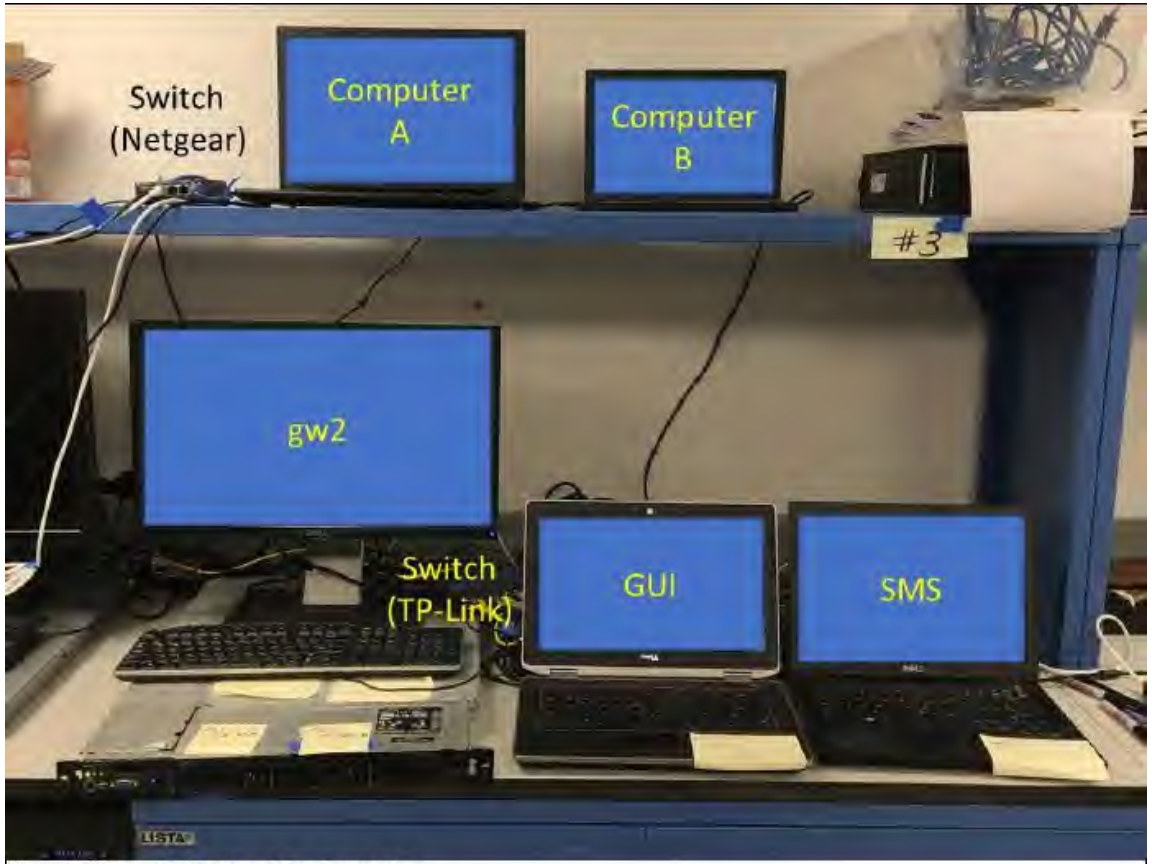
’856 Patent:	Check Point R77
24. [a] A packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;	
[b] identify packets comprising unencrypted data;	
[c] identify packets comprising encrypted data;	
[d] 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;	
[e] 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	
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	
[g] 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.	

’856 Patent Analysis – Check Point R77

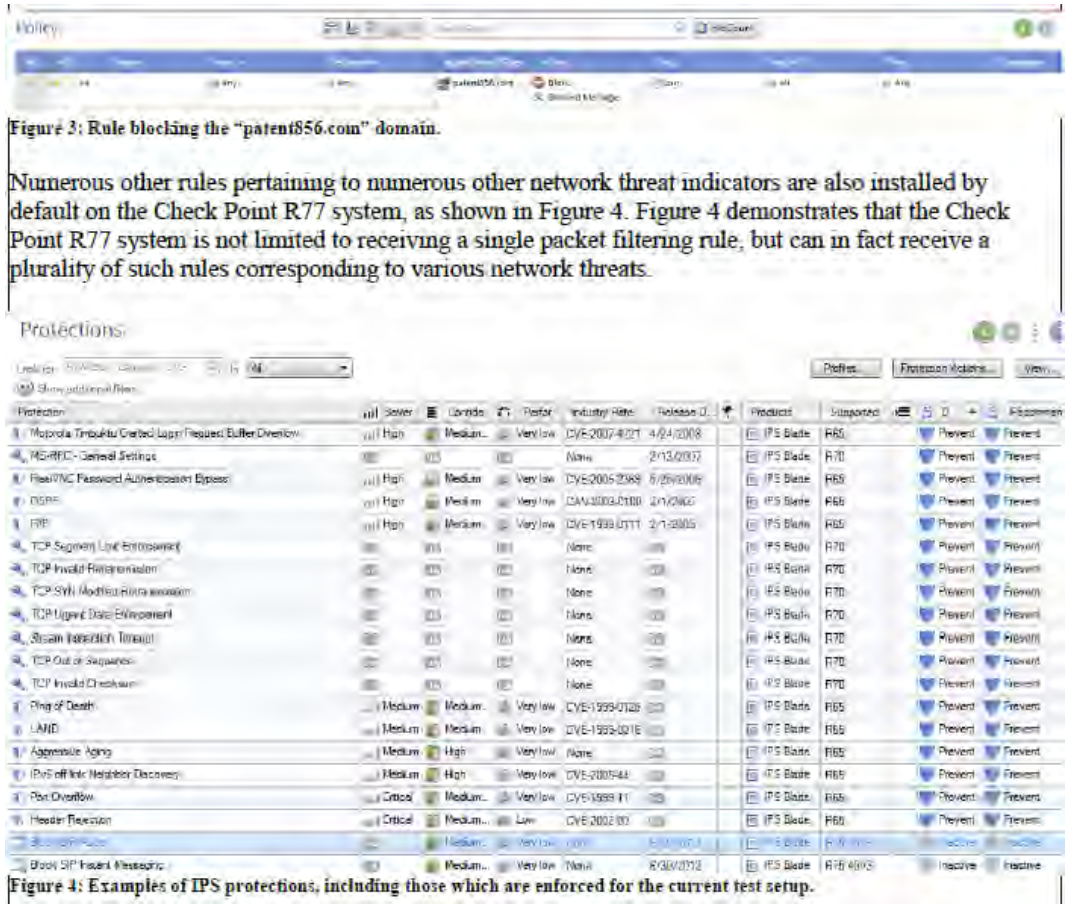
’856 Patent:	Check Point R77
24. **[a]** A packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;	 Figure 1: Network diagram of test setup

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 250

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24. [a] 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;	 Figure 2: Image of test network hardware setup.

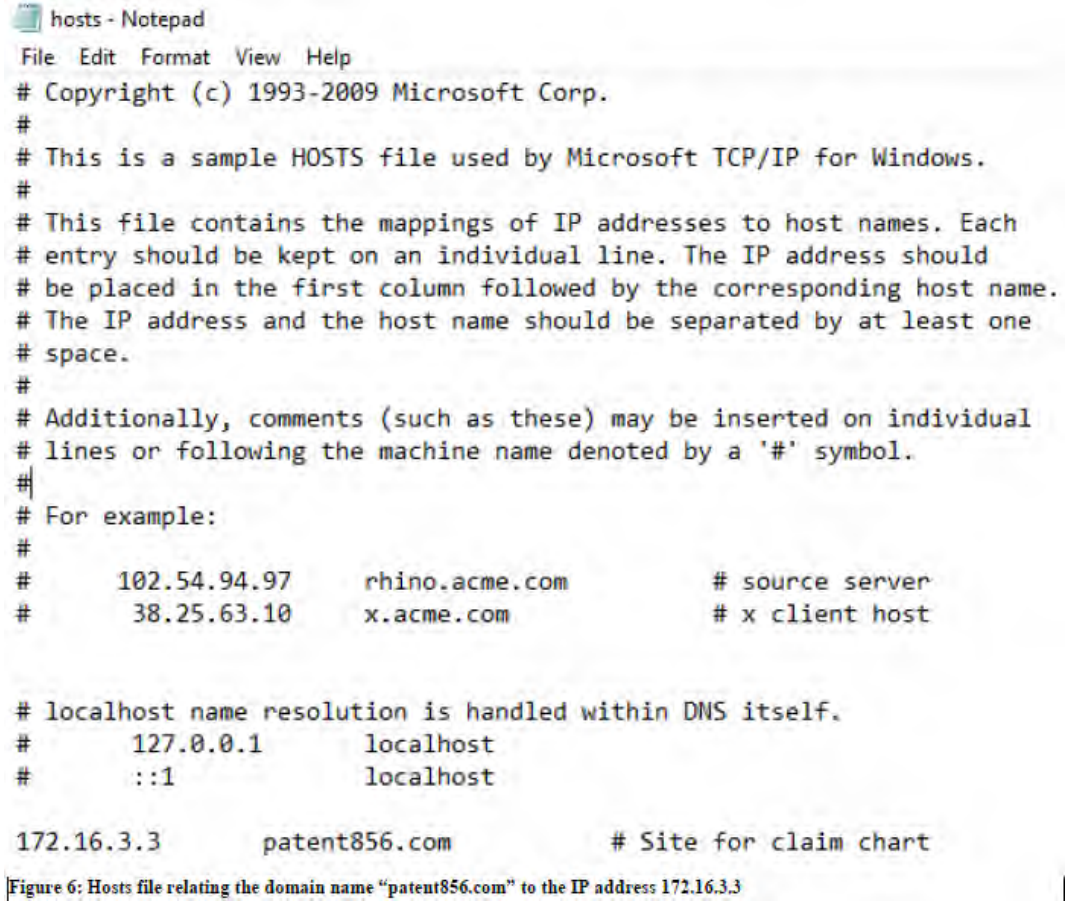
’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24. [a] 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;	 **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.**

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24. [a] 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;	 Figure 5: Screenshot showing a final allow rule, which applies to any traffic that is not blocked by the other rules.

’856 Patent Analysis – Check Point R77

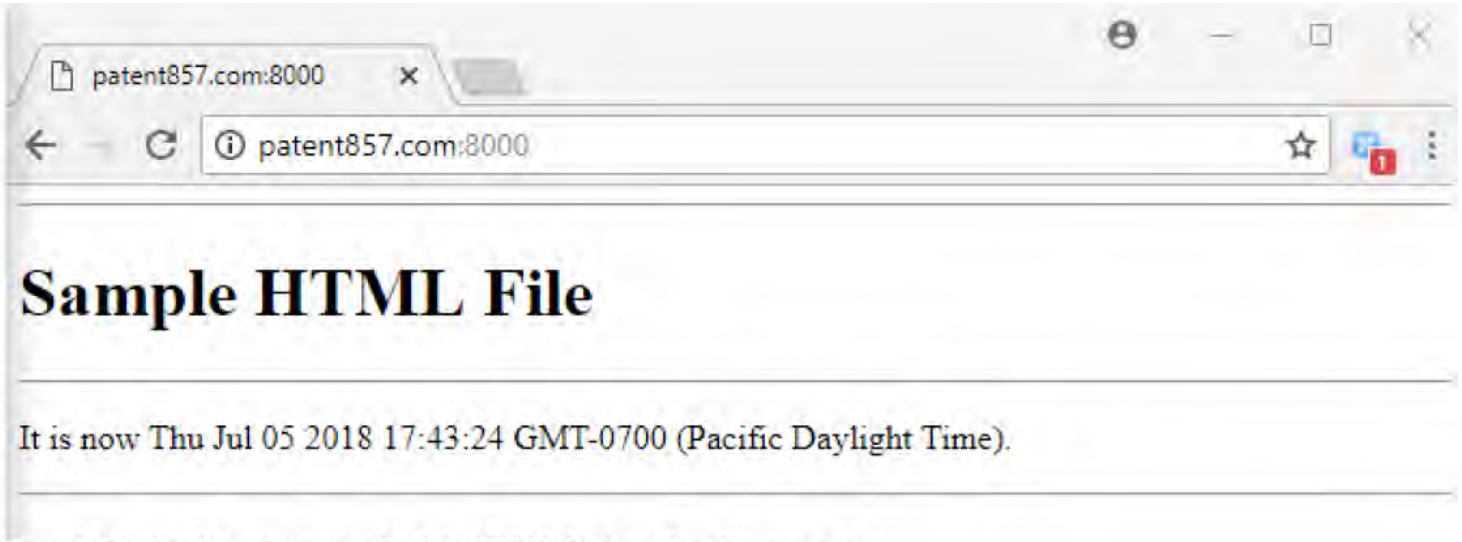
’856 Patent:	Check Point R77
24. [a] A packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;	 Figure 6: Hosts file relating the domain name “patent856.com” to the IP address 172.16.3.3

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 254

’856 Patent Analysis – Check Point R77

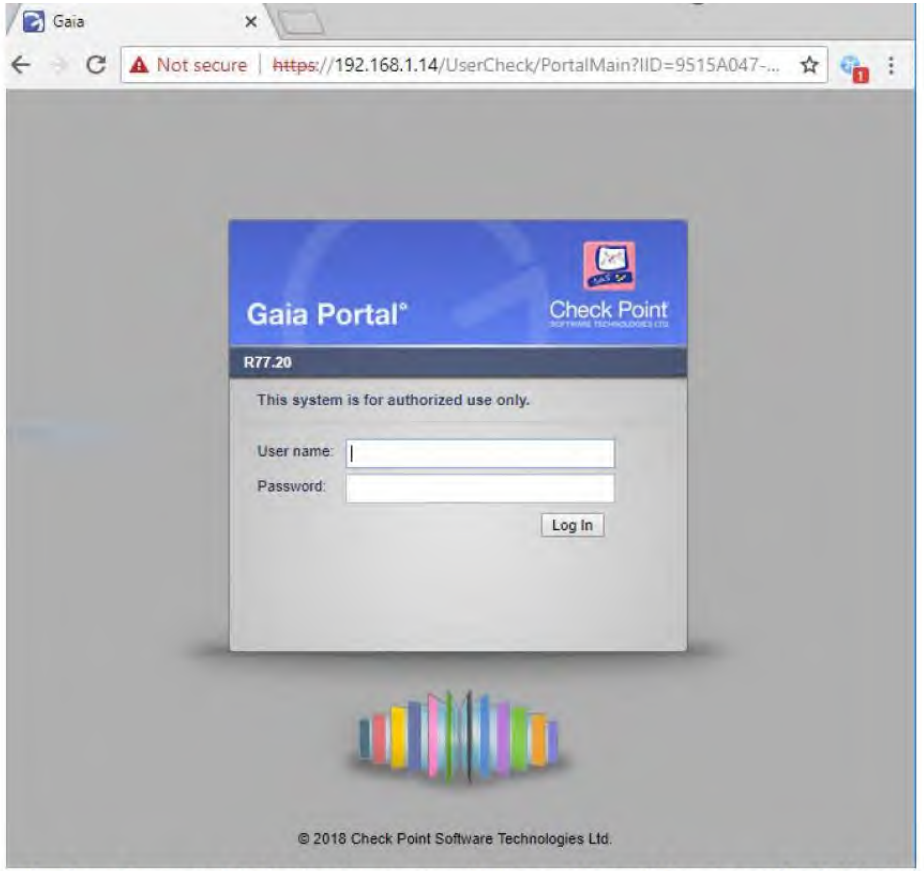
’856 Patent:	Check Point R77
24. [a] A packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;	 Figure 7: Hosting on Port 8000 of Computer A  Figure 8: Initial test set up for the hosts file to associate the domain name “patent857.com” with IP address 172.16.3.3

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24. [a] 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;	 **Figure 9: Display from Computer B of the HTML file hosted on Computer A**  **Figure 10: Modification to the hosts file to associate the domain name “patent856.com” with the IP address 172.16.3.3.**

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 256

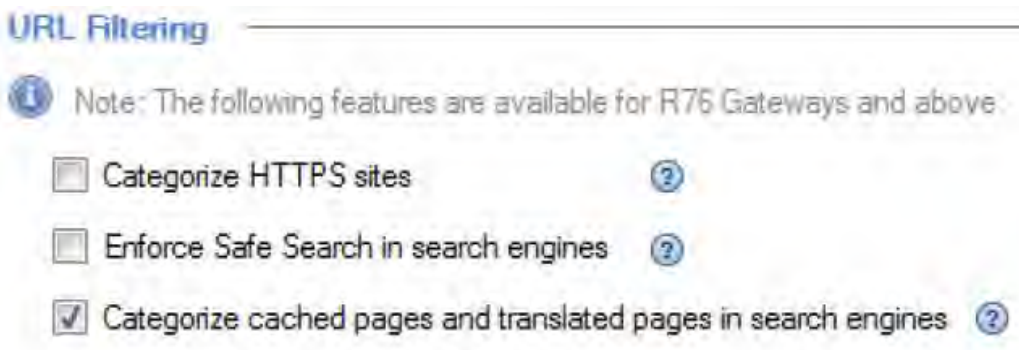
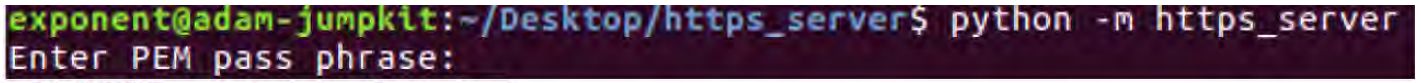
’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24. [a] 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;	 **Figure 11: Screenshot from Computer A indicating that access to the “patent856.com” domain was blocked by the gateway.**

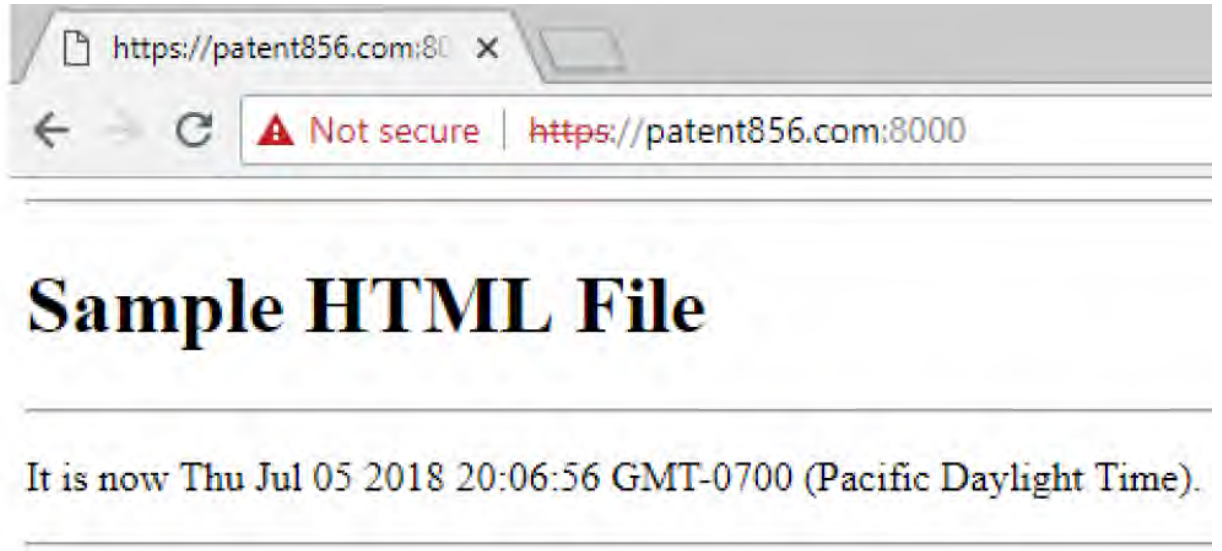
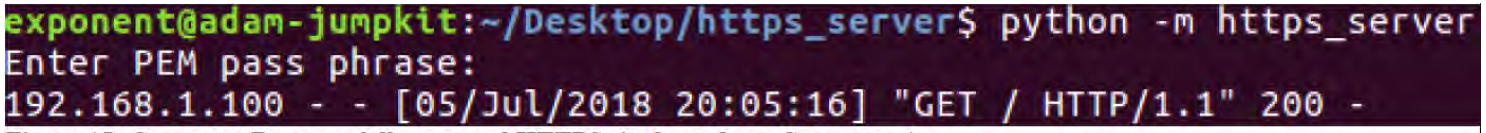
Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent:	Check Point R77
24. [a] 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;	✓
[b] identify packets comprising unencrypted data;	
[c] identify packets comprising encrypted data;	
[d] 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;	
[e] 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	
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	
[g] 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.	

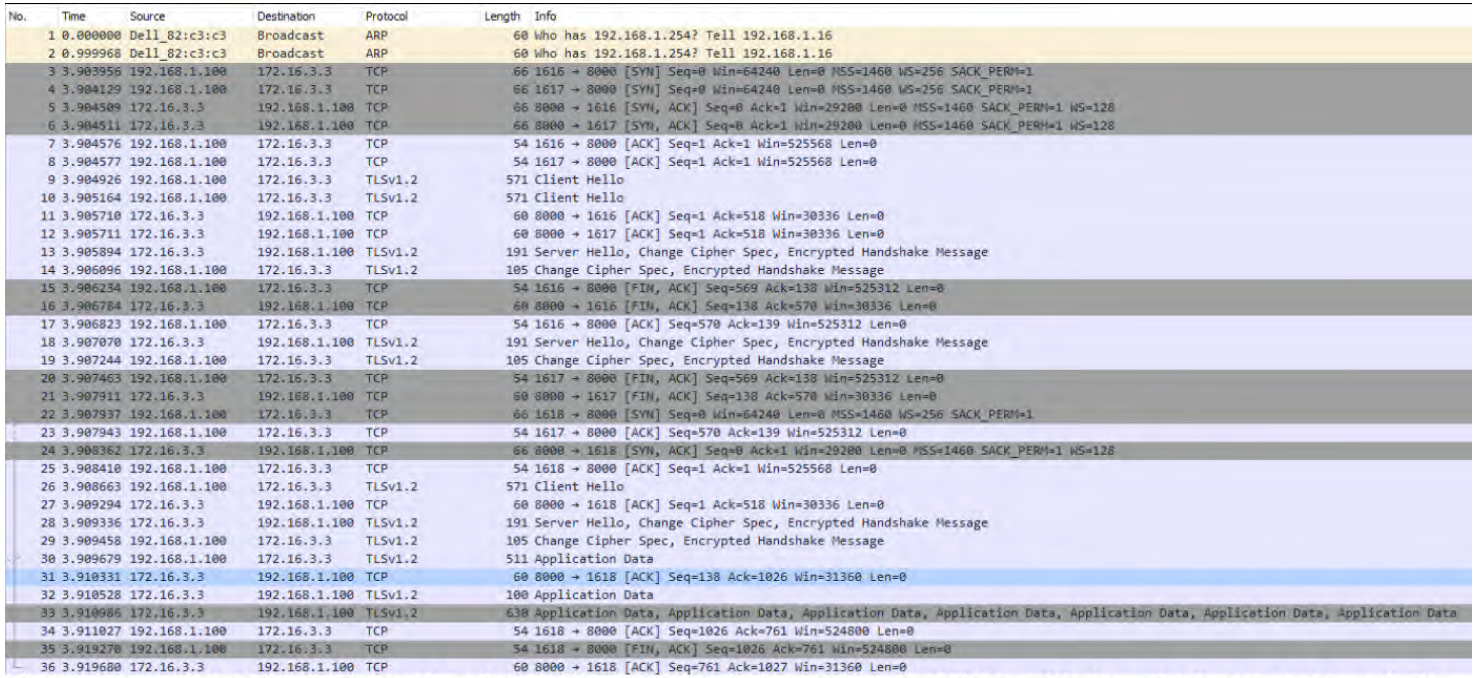
’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… **[b]** identify packets comprising unencrypted data;	 **Figure 12: HTTPS sites are not categorized.**  **Figure 13: HTTPS server hosted on Computer A**

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… **[b]** identify packets comprising unencrypted data;	 **Figure 14: Successful loading of HTTPS site**  **Figure 15: Computer B successfully accessed HTTPS site hosted son Computer A.**

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… **[b]** identify packets comprising unencrypted data;	

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	3.905894	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	3.907911	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	3.919270	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

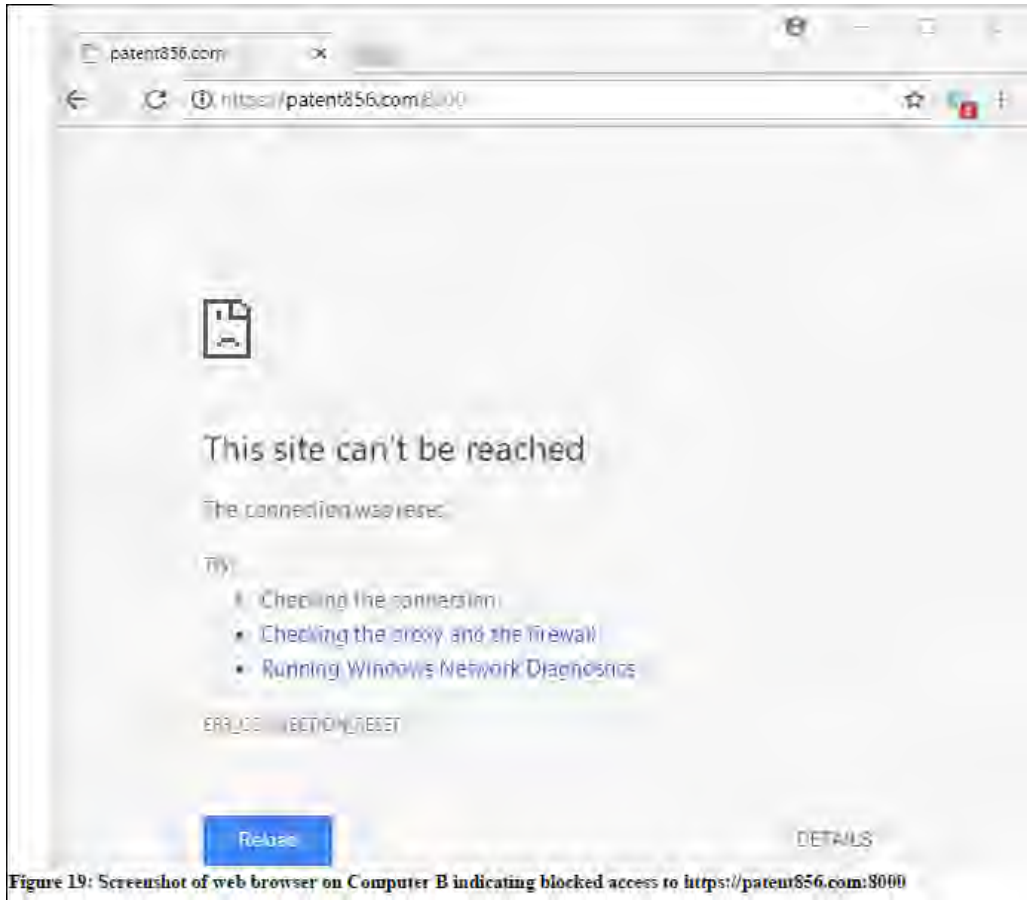
Figure 16: Screenshot from Wireshark packet capture session showing a successful TLS handshake and subsequent transmission of encrypted application data.

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77

24… **[b]** identify packets comprising unencrypted data;	URL Filtering
	Note: The following features are available for R76 Gateways and above.
	☑ Categorize HTTPS sites
	☐ Enforce Safe Search in search engines
	☑ Categorize cached pages and translated pages in search engines
	Figure 17: “Categorize HTTPS sites” blocks sites with the HTTPS domain name.
	`exponent@adam-jumpkit:~/Desktop/https_server$ python -m https_server`
	`Enter PEM pass phrase:`
	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.

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… **[b]** identify packets comprising unencrypted data;	 Figure 19: Screenshot of web browser on Computer B indicating blocked access to https://patent856.com:8000

’856 Patent Analysis – Check Point R77

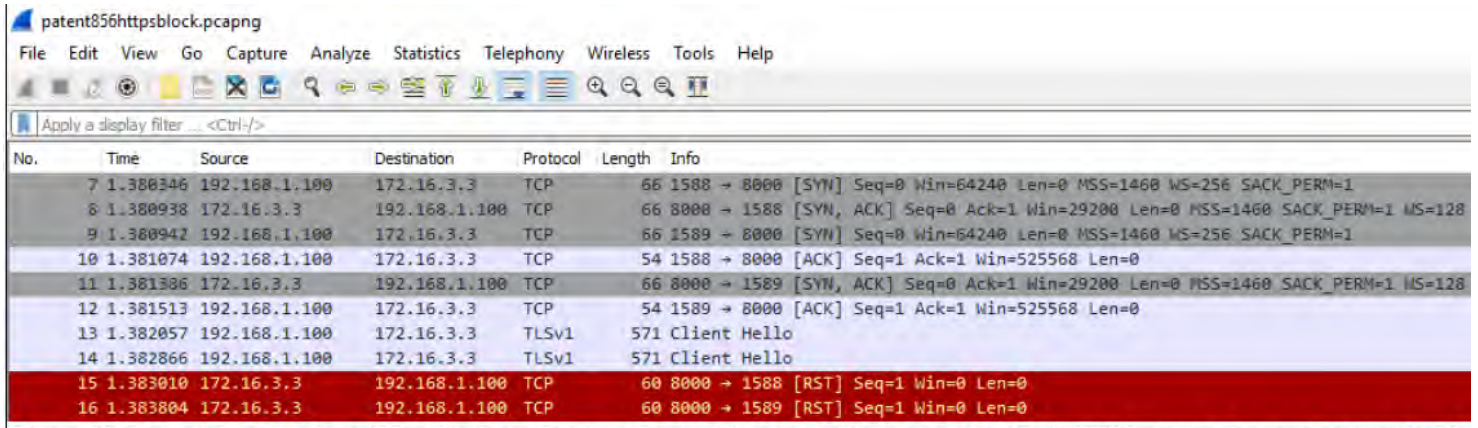
’856 Patent:	Check Point R77
24… **[b]** identify packets comprising unencrypted data;	

Figure 20: Screen Capture from Wireshark session running on Computer B showing that the HTTPS server does not respond with a “Server Hello.”

Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent:	Check Point R77
24. [a] 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;	✓
[b] identify packets comprising unencrypted data;	✓
[c] identify packets comprising encrypted data;	
[d] 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;	
[e] 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	
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	
[g] 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.	

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… [c] identify packets comprising encrypted data;	**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.  ***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.

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… [c] identify packets comprising encrypted data;	You can enable HTTPS traffic inspection on Security Gateways to inspect traffic that is encrypted by the Secure Sockets Layer (SSL) protocol. 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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 267

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… [c] identify packets comprising encrypted data;	**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.

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… [c] identify packets comprising encrypted data;	You must enable HTTPS inspection on each Security Gateway. From **Security Gateway** > **HTTPS Inspection** > **Step 3** > Select **Enable HTTPS Inspection**.

Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent:	Check Point R77
24. **[a]** 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;	✓
[b] identify packets comprising unencrypted data;	✓
[c] identify packets comprising encrypted data;	✓
[d] 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;	
[e] 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	
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	
[g] 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.	

’856 Patent Analysis – Check Point R77

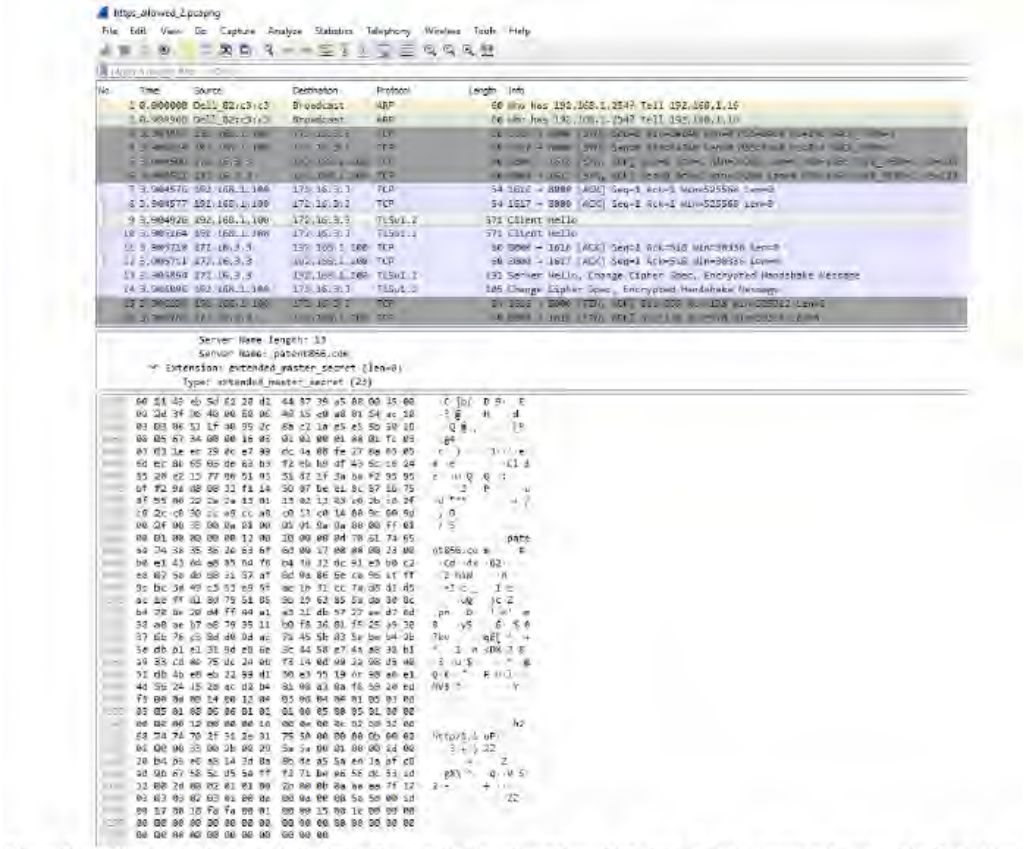
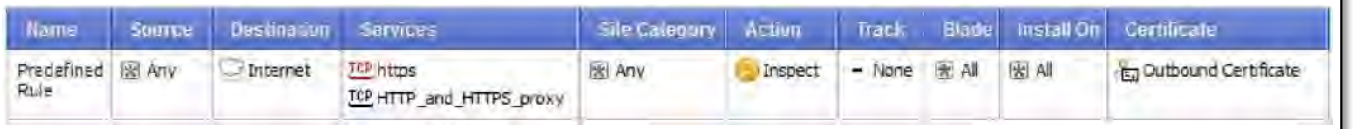
’856 Patent:	Check Point R77
24… **[d]** determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;	

Figure 21: “Client Hello” packet during https handshake, showing “Patent856.com” as an unencrypted segment in the packet (lines 00c0 and 00d0).

Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent:	Check Point R77
24. [a] 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;	✓
[b] identify packets comprising unencrypted data;	✓
[c] identify packets comprising encrypted data;	✓
[d] 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;	✓
[e] 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	
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	
[g] 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.	

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… **[e]** 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	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). **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. 

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 273

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… **[e]** 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	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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 274

Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent:	Check Point R77
24. [a] 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;	✓
[b] identify packets comprising unencrypted data;	✓
[c] identify packets comprising encrypted data;	✓
[d] 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;	✓
[e] 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	✓
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	
[g] 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.	

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… [f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	**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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 276

Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent:	Check Point R77
24. [a] 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;	✓
[b] identify packets comprising unencrypted data;	✓
[c] identify packets comprising encrypted data;	✓
[d] 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;	✓
[e] 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	✓
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	✓
[g] 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.	

’856 Patent Analysis – Check Point R77

’856 Patent:	Check Point R77
24… [g] 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.	**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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 278

Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent:	Check Point R77
24. [a] 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;	✓
[b] identify packets comprising unencrypted data;	✓
[c] identify packets comprising encrypted data;	✓
[d] 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;	✓
[e] 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	✓
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	✓
[g] 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.	✓

Check Point R77 Invalidates the ’856 Patent, Claim 24

’856 Patent, Claim 24	’856 Patent, Claim 25
24. [a] **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;	**25**. [a] 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;
[b] identify packets comprising unencrypted data;	[b] identify packets comprising unencrypted data;
[c] identify packets comprising encrypted data;	[c] identify packets comprising encrypted data;
[d] 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;	[d] 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;
[e] 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	[e] 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
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and
[g] 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.	[g] 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.

Check Point R77 Invalidates the ’856 Patent, Claim 25

’856 Patent:	Check Point R77
25. [a] 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;	✓
[b] identify packets comprising unencrypted data;	✓
[c] identify packets comprising encrypted data;	✓
[d] 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;	✓
[e] 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	✓
[f] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	✓
[g] 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.	✓

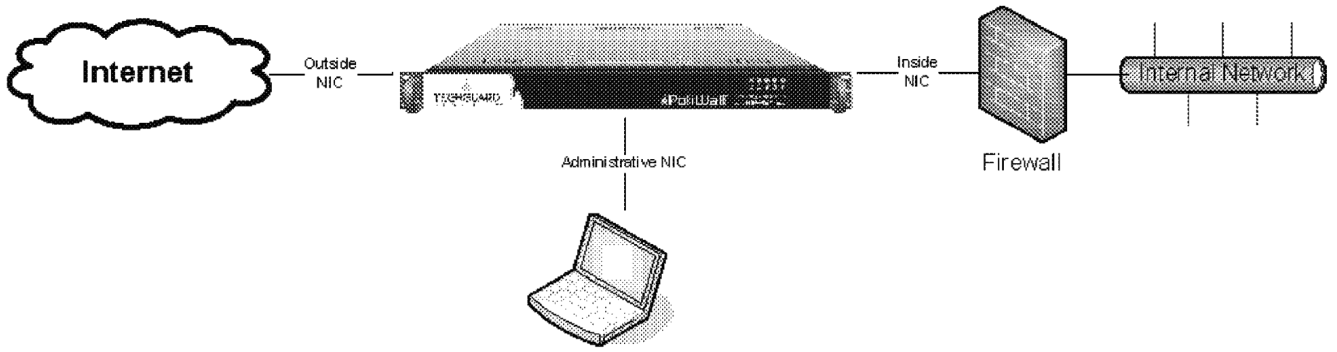

PoliWall™

PoliWall™ Invalidates the ’205 Patent Claims 17, 33

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	
[b] receive a plurality of dynamic security policies from the security policy management server,	
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – PoliWall™

’205 Patent:	PoliWall™
17. **[a]** 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:	PoliWall™ The following diagram shows the typical placement of the PoliWall in a network between the Internet border router and your firewall. 

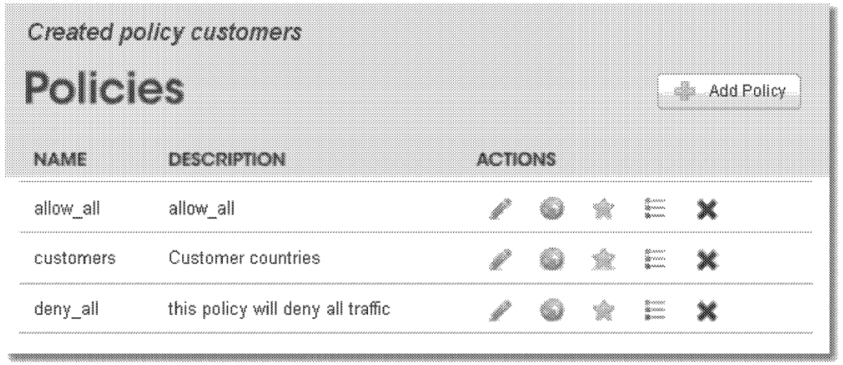
’205 Patent Analysis – PoliWall™

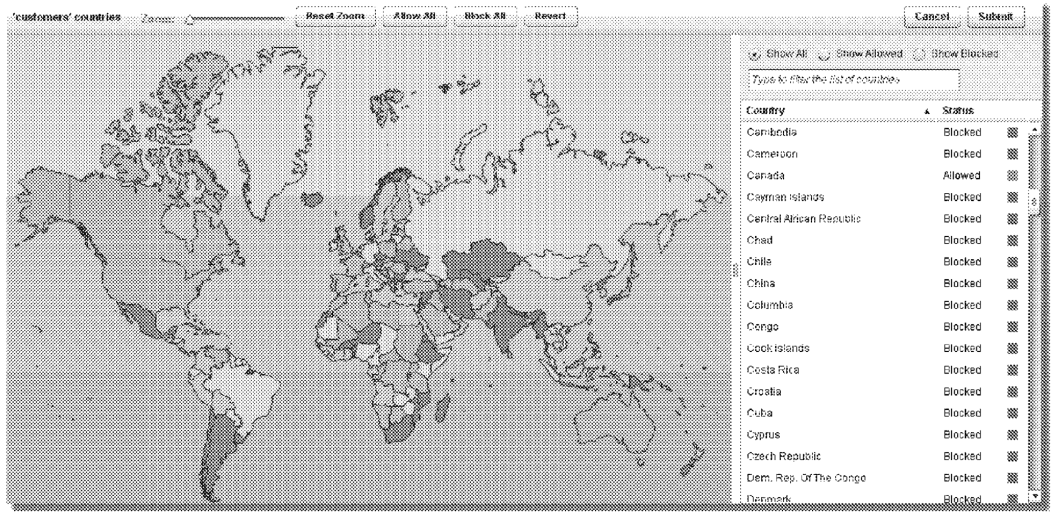
’205 Patent:	PoliWall™
17. [a] A system, comprising: a security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to:	**2.1 Initial configuration** * * * To configure the PoliWall, you need a standard personal computer with a web browser that supports Adobe Flash. Browsers tested include Microsoft Internet Explorer 8 and Mozilla Firefox 3.5 and 3.6. You may use any operating system that supports one of these browsers, such as Microsoft Windows, Mac OS X, and Linux.

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – PoliWall™

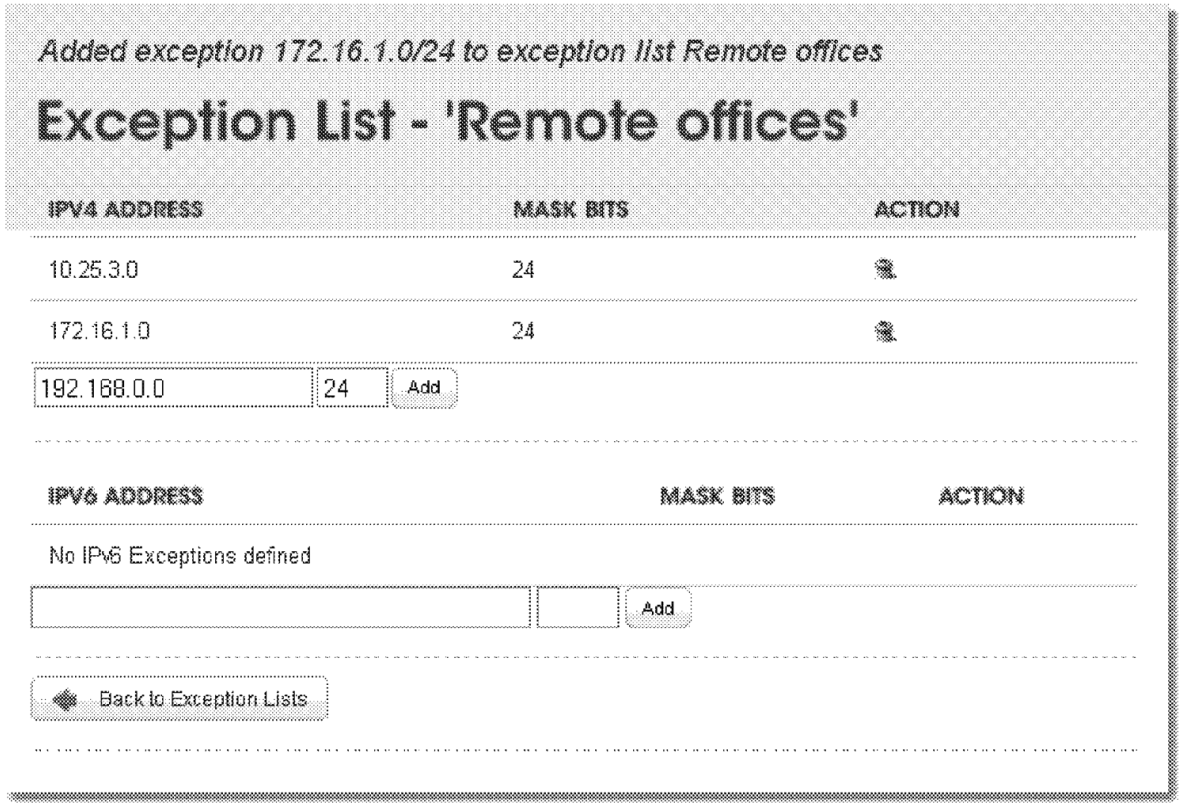
’205 Patent:	PoliWall™
17. **[b]** receive a plurality of dynamic security policies from the security policy management server,	



PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

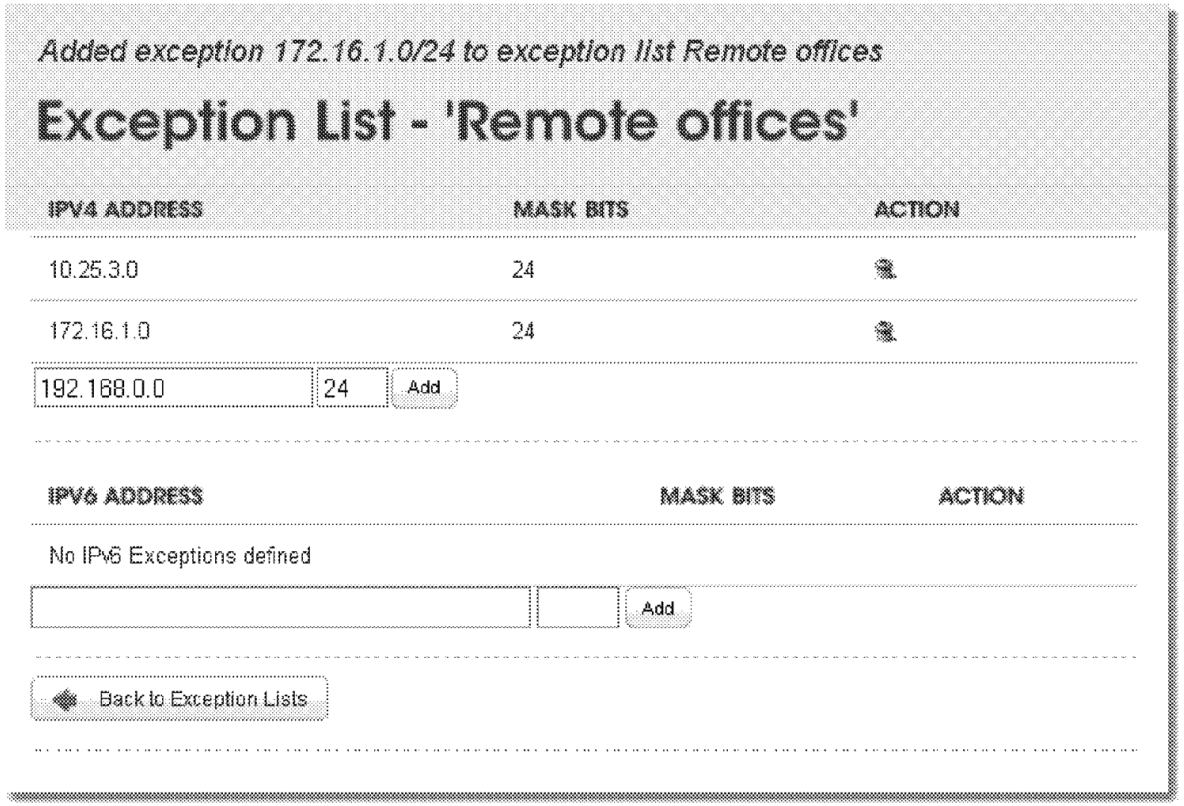
’205 Patent Analysis – PoliWall™

’205 Patent:	PoliWall™
17. [c] 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;	 Click the **Add** button enter an exception, and click the trashcan icon to delete an exception.

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

’205 Patent Analysis – PoliWall™

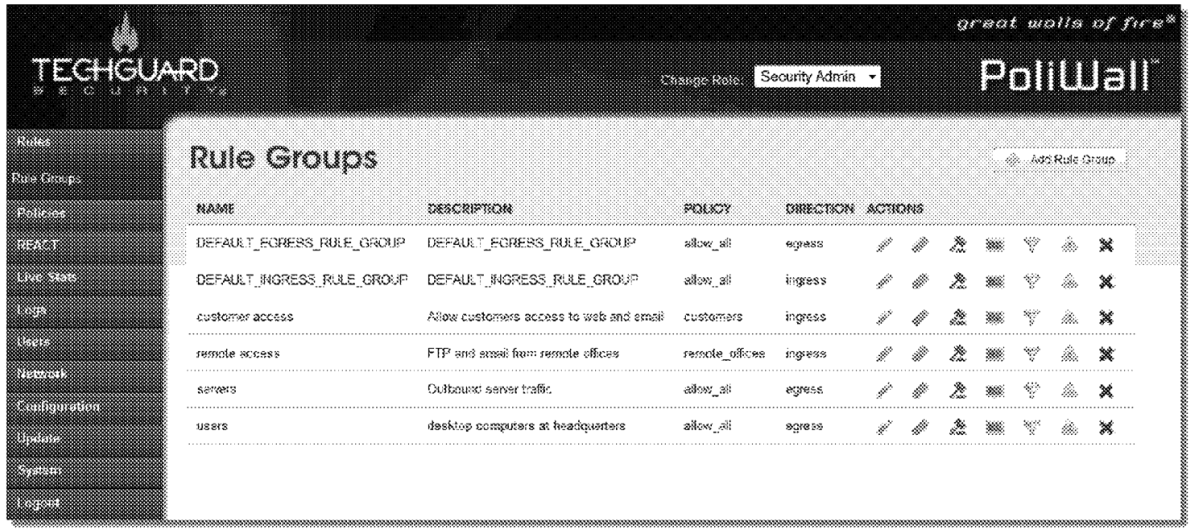
’205 Patent:	PoliWall™
17. **[d]** receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	

Click the **Add** button enter an exception, and click the trashcan icon to delete an exception.

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

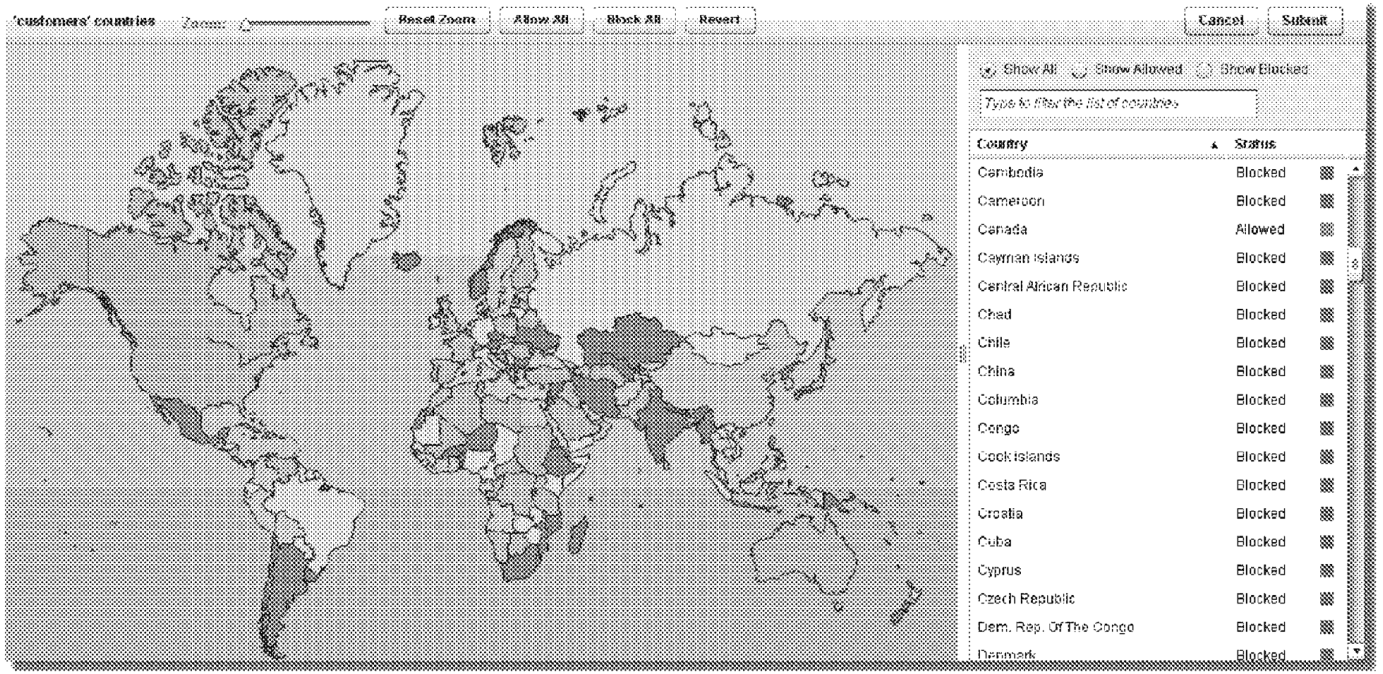
’205 Patent Analysis – PoliWall™

’205 Patent:	PoliWall™
17. **[e]** receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	 **Rule Groups** are the core of the PoliWall's packet filtering system. The PoliWall examines rule groups to determine which Internet packets to drop or transmit. With rule groups you determine what Internet services you will offer on your network, and what kind of services your local users can access on the outside. You need to configure at least one Rule Group before you can place the PoliWall into your network. You can also configure bandwidth limits in Rule Groups; or if traffic exceeds a limit, you can **throttle** the traffic and send an **alert** to your network management system. Rule Groups also include **Quality of Service** (**QoS**) settings, where you can give some traffic priority over others.

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

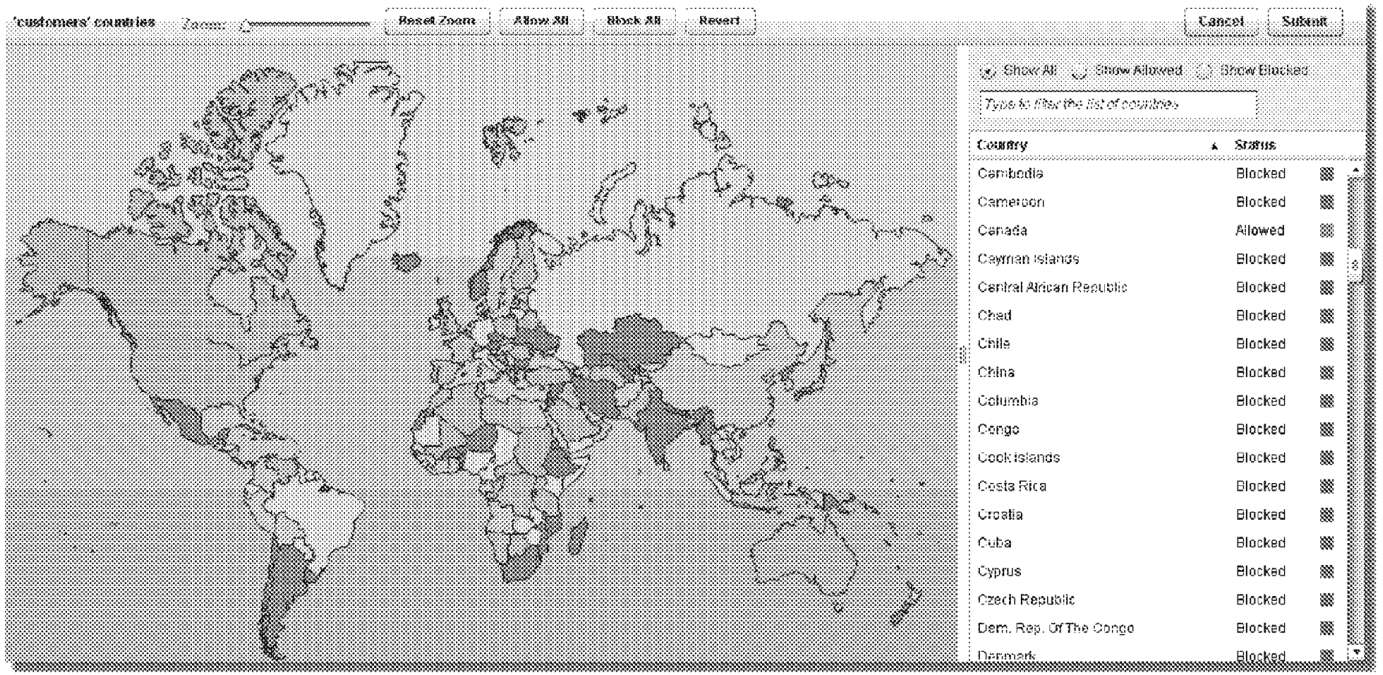
’205 Patent Analysis – PoliWall™

’205 Patent:	PoliWall™
17. [f] 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;	

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	
[h] 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.	

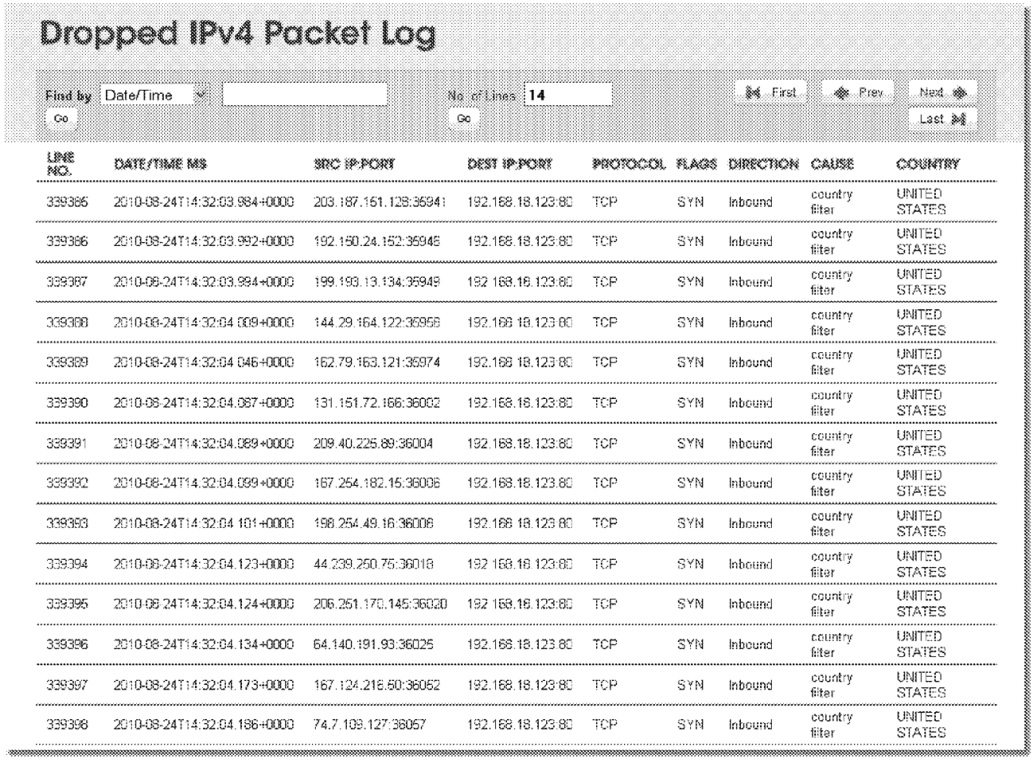
’205 Patent Analysis – PoliWall™

’205 Patent:	PoliWall™
17. [g] receive packets associated with a network protected by the packet security gateway; and	

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	

’205 Patent Analysis – PoliWall™

’205 Patent:	PoliWall™
17. [h] 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.	**3.5.1 IP Packet Logs**  Dropped IPv4 Packet Log Find by Date/Time Go — No. of Lines 14 Go — First Prev Next Last LINE NO. | DATE/TIME MS | SRC IP:PORT | DEST IP:PORT | PROTOCOL | FLAGS | DIRECTION | CAUSE | COUNTRY 339385 | 2010-08-24T14:32:03.984+0000 | 203.187.161.128:35941 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339386 | 2010-08-24T14:32:03.992+0000 | 192.150.24.152:35945 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339387 | 2010-08-24T14:32:03.994+0000 | 199.193.13.134:35949 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339388 | 2010-08-24T14:32:04.009+0000 | 144.29.164.122:35956 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339389 | 2010-08-24T14:32:04.046+0000 | 162.79.163.121:35974 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339390 | 2010-08-24T14:32:04.087+0000 | 131.151.72.166:36002 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339391 | 2010-08-24T14:32:04.089+0000 | 209.40.225.89:36004 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339392 | 2010-08-24T14:32:04.099+0000 | 167.254.182.15:36006 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339393 | 2010-08-24T14:32:04.101+0000 | 198.254.49.16:36008 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339394 | 2010-08-24T14:32:04.123+0000 | 44.239.250.75:36018 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339395 | 2010-08-24T14:32:04.124+0000 | 206.251.170.145:36020 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339396 | 2010-08-24T14:32:04.134+0000 | 64.140.191.93:36025 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339397 | 2010-08-24T14:32:04.173+0000 | 167.124.216.50:36052 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES 339398 | 2010-08-24T14:32:04.186+0000 | 74.7.109.127:36057 | 192.168.18.123:80 | TCP | SYN | Inbound | country filter | UNITED STATES The **Dropped IPv4 Packet Log** and the **Dropped IPv6 Packet Log** screens show you information on data packets blocked by the PoliWall.

PoliWall™ Invalidates the ’205 Patent, Claim 17

’205 Patent:	PoliWall™
17. [a] 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:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	✓

’205 Patent, Claims 17 and 33 Comparison

17. 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:	33. 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:
receive a plurality of dynamic security policies from the security policy management server,	receive a plurality of dynamic security policies from the security policy management server;
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;	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;
receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;
receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;
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;	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;
receive packets associated with a network protected by the packet security gateway; and	receive packets associated with a network protected by the packet security gateway; 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.	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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 302

PoliWall™ Invalidates the ’205 Patent, Claim 33

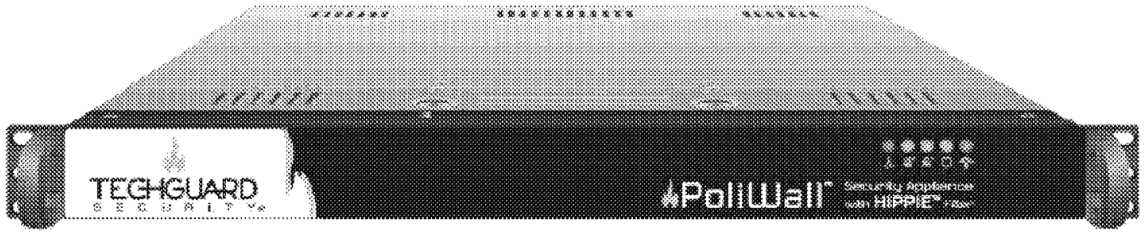
’205 Patent:	PoliWall™
33. [a] One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:	✓
[b] receive a plurality of dynamic security policies from the security policy management server,	✓
[c] 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;	✓
[d] receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;	✓
[e] receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;	✓
[f] 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;	✓
[g] receive packets associated with a network protected by the packet security gateway; and	✓
[h] 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.	✓

PoliWall™ Invalidates the ’722 Patent Claim 1

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1. **[a]** 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 **PoliWall-CCF™** resides between your firewall and Internet connection, where it acts as an OSI Level 2 network bridge, and so is invisible to the Internet. The PoliWall incorporates the unique **HIPPIE™** (High-speed Internet Protocol Packet Inspection Engine) technology, which determines the country of origin of each packet, and filters inbound and outbound packets at wire speeds. You can create many filters for the PoliWall, based on country and IP network, and you can add exceptions to these filters. The PoliWall can automatically download updated lists of known threats such as spammers and botnets. You can define the Quality of Service for countries and networks of your choosing; you can also throttle traffic according to custom filters. You can define alerts, and automatically throttle suspicious traffic. You configure the PoliWall from a standard web browser, and this administration function is protected by multiple levels of security including Public Key Certificates, trusted network lists, and administrator passwords. The device supports both IPv4 and IPv6, and can be managed via SNMP.

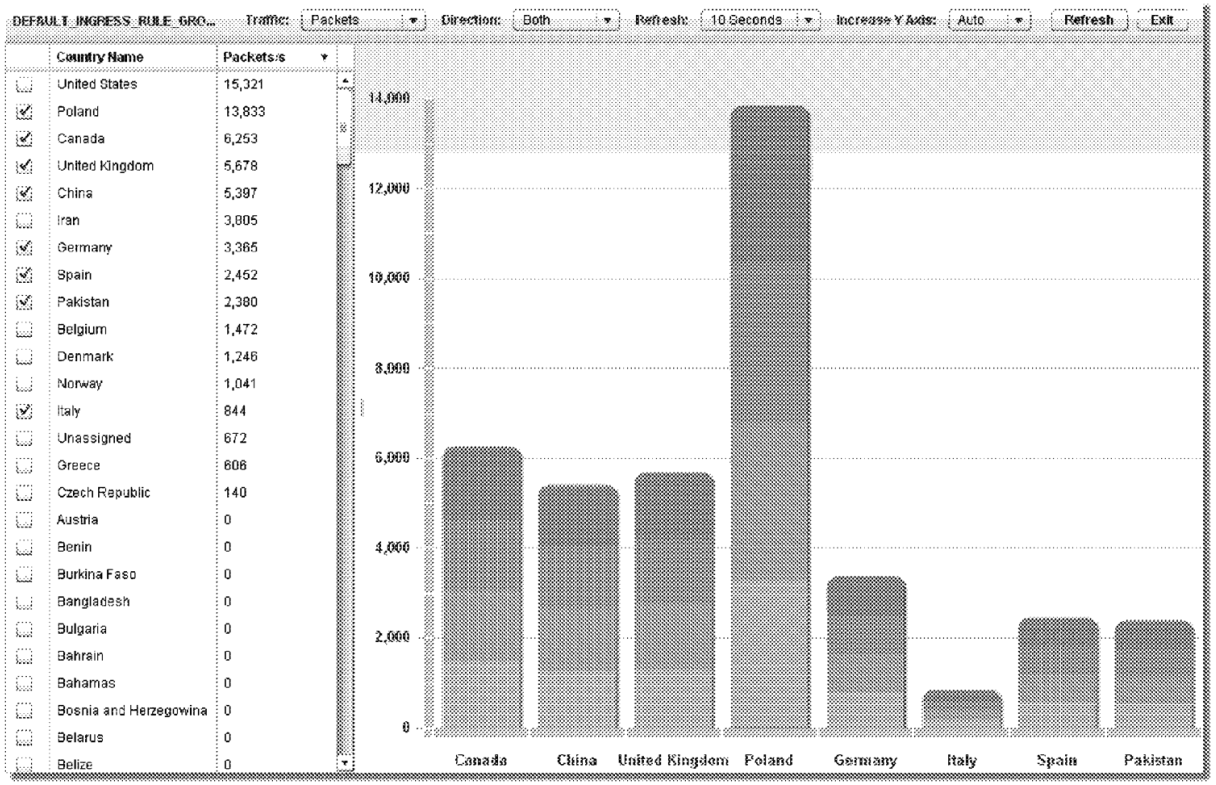
’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1. **[a]** 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;	***HIPPIE™ Filter*** HIPPIE is a country code/Internet Protocol address engine that rapidly determines the country of origin for incoming packets, and the destination country of outgoing packets. You create maps by specifying one or more countries that should be blocked or allowed. You may also specify additional allow/deny rules for IP networks or addresses with as much granularity as desired across the entire IP address space. Changes to this filter can be automatically downloaded to the PoliWall-CCF.

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

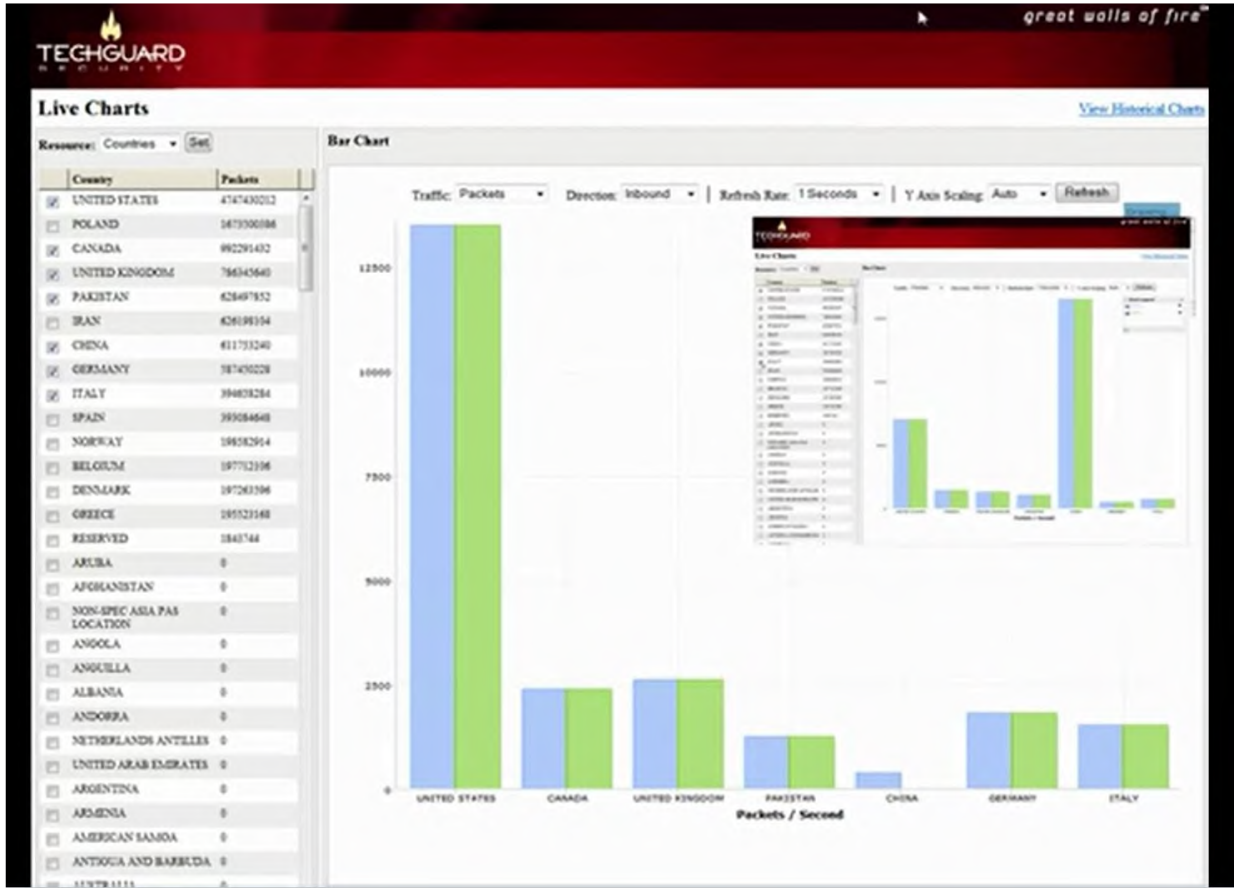
’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… **[b]** receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	View Real-time statistics for your **Rule Groups**. Click any **View Stats** button to pull up a graph of traffic. 

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… [c] 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;	

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

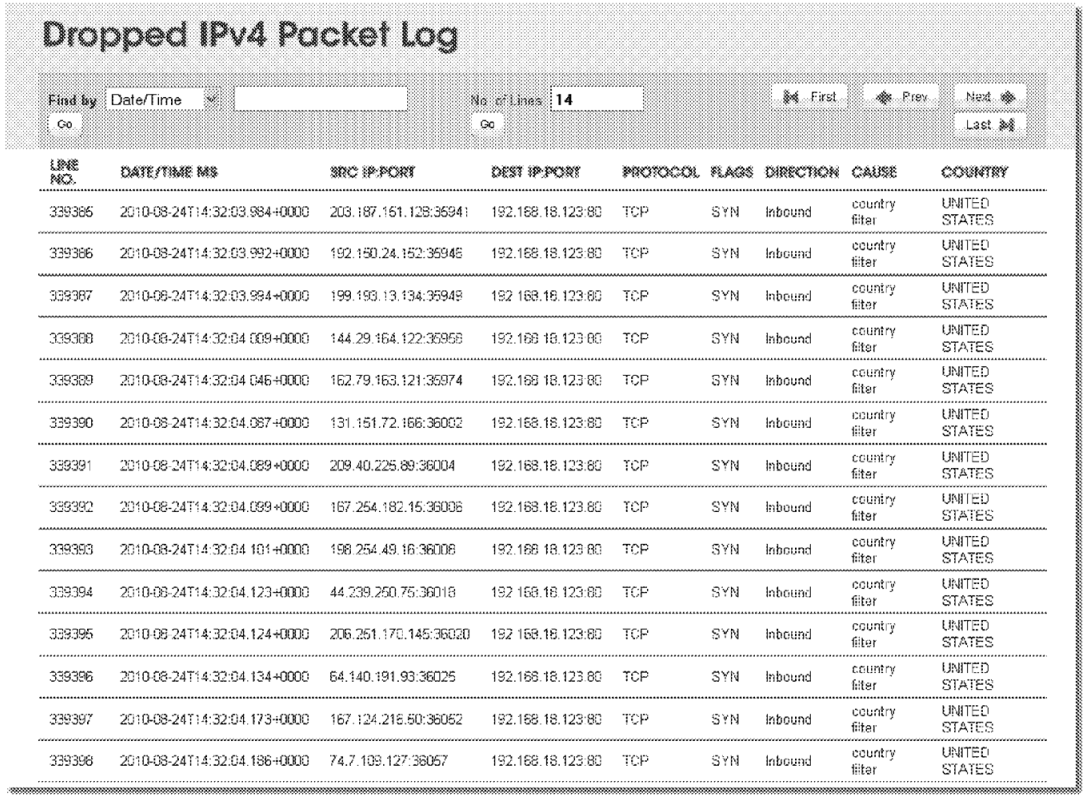
’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… [d] 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;	**Live Stats** provide a graphical view of the traffic currently going through the PoliWall, after filtering. The table on the left can be sorted by country name or by traffic. You can select countries from the table and view their traffic on a bar graph on the right. Here are your options: • **Traffic**: Packets, Bandwidth used (megabits per second), and Connections • **Direction**: Inbound, Outbound, or both • **Refresh**: Rate of chart update from 1 second to 1 minute. • **Increase Y Axis**: Either fix the scale of the axis, or allow it to resize automatically.

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… **[e]** 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;	

Dropped IPv4 Packet Log

Find by Date/Time Go No. of Lines 14 Go First Prev Next Last

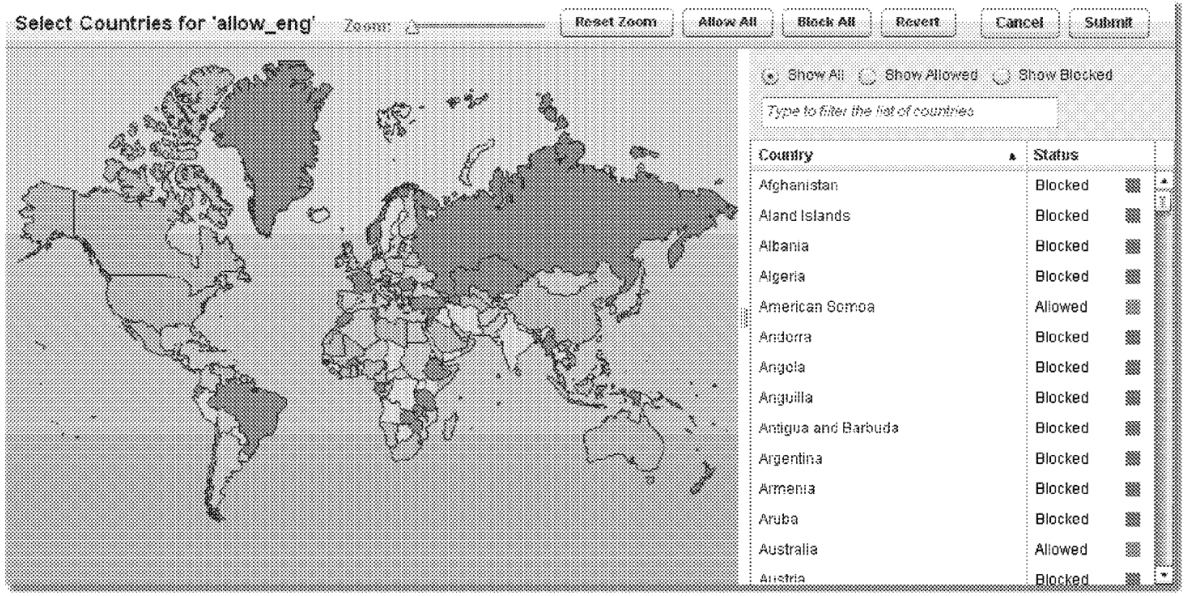
LINE NO.	DATE/TIME MS	SRC IP:PORT	DEST IP:PORT	PROTOCOL	FLAGS	DIRECTION	CAUSE	COUNTRY
339385	2010-08-24T14:32:03.984+0000	203.187.151.128:36941	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339386	2010-08-24T14:32:03.992+0000	192.150.24.152:35945	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339387	2010-08-24T14:32:03.994+0000	199.193.13.134:35949	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339388	2010-08-24T14:32:04.009+0000	144.29.164.122:35956	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339389	2010-08-24T14:32:04.046+0000	162.79.163.121:35974	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339390	2010-08-24T14:32:04.087+0000	131.151.72.166:36002	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339391	2010-08-24T14:32:04.089+0000	209.40.225.89:36004	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339392	2010-08-24T14:32:04.099+0000	167.254.182.15:36006	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339393	2010-08-24T14:32:04.101+0000	198.254.49.16:36008	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339394	2010-08-24T14:32:04.123+0000	44.239.250.75:36018	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339395	2010-08-24T14:32:04.124+0000	206.251.170.145:36020	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339396	2010-08-24T14:32:04.134+0000	64.140.191.93:36025	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339397	2010-08-24T14:32:04.173+0000	167.124.216.60:36052	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339398	2010-08-24T14:32:04.186+0000	74.7.109.127:36057	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES

The **Dropped IPv4 Packet Log** and the **Dropped IPv6 Packet Log** screens show you information on data packets blocked by the PoliWall.

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

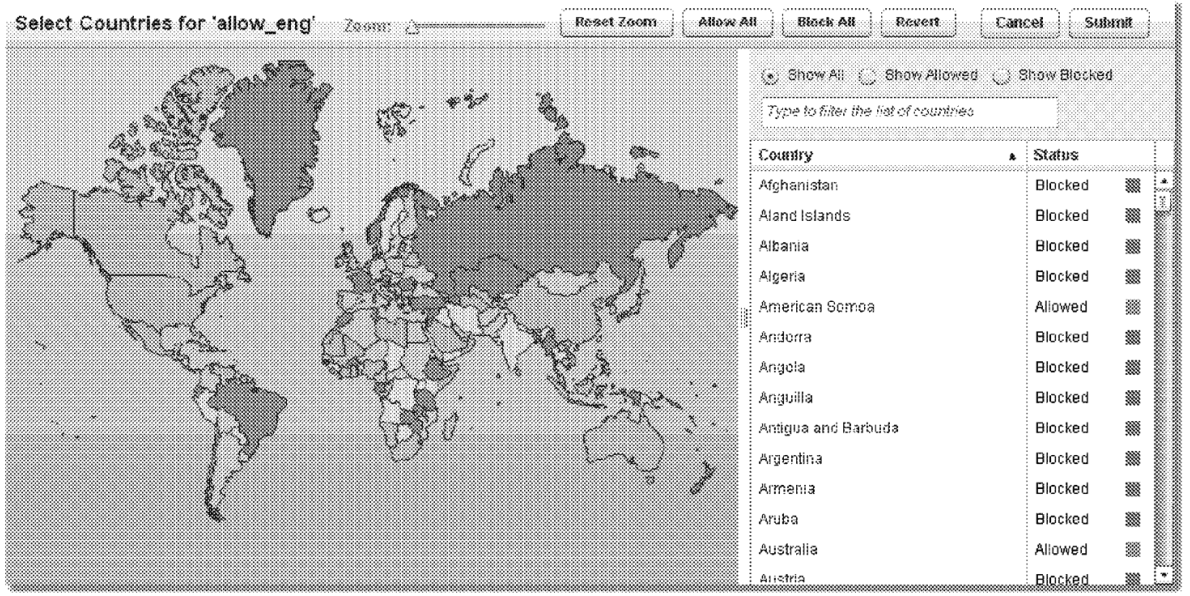
’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… [f] 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	The **World Map** lets you allow or deny Internet traffic to the various countries of the world.  Click on an country to select it: green shows allowed countries, gray shows those that are blocked. Alternatively, select countries from the list on the right side of the screen. Click on **Submit** to save your changes, or click on **Revert** to undo your changes. Note: you need the **Adobe Flash** plug-in on your web browser to display the world map. You can download a copy of Flash here: http://get.adobe.com/flashplayer.

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

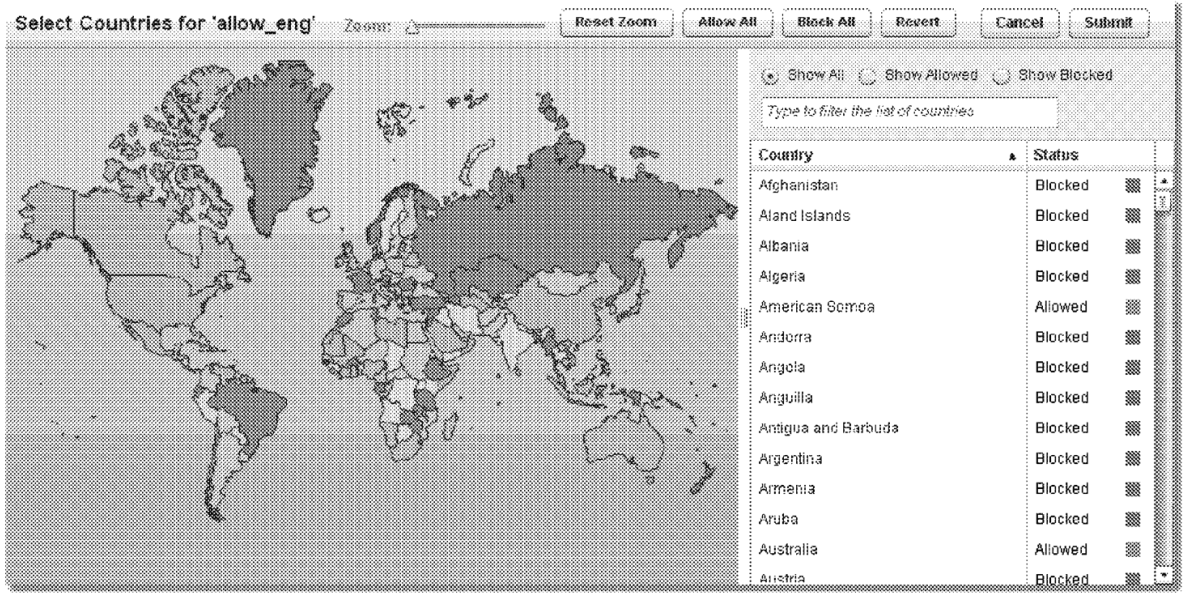
’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… [g] 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 **World Map** lets you allow or deny Internet traffic to the various countries of the world.  Click on an country to select it: green shows allowed countries, gray shows those that are blocked. Alternatively, select countries from the list on the right side of the screen. Click on **Submit** to save your changes, or click on **Revert** to undo your changes. Note: you need the **Adobe Flash** plug-in on your web browser to display the world map. You can download a copy of Flash here: http://get.adobe.com/flashplayer.

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

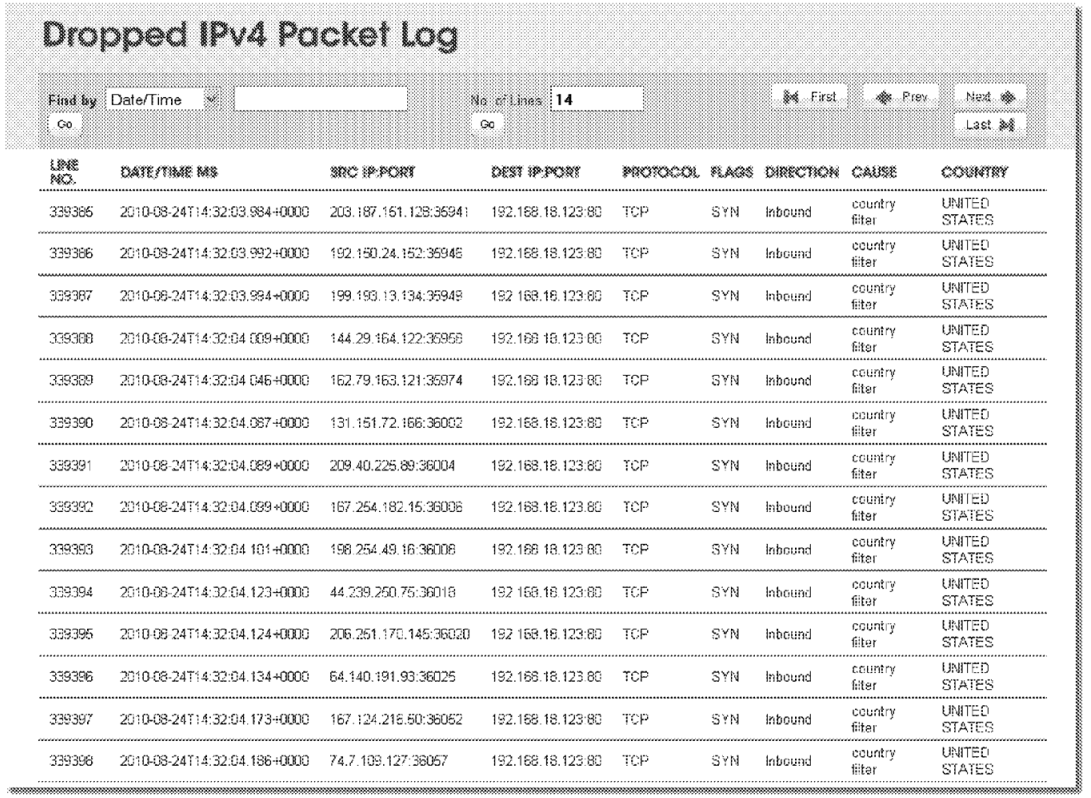
’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… [h] 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 **World Map** lets you allow or deny Internet traffic to the various countries of the world.  Click on an country to select it: green shows allowed countries, gray shows those that are blocked. Alternatively, select countries from the list on the right side of the screen. Click on **Submit** to save your changes, or click on **Revert** to undo your changes. Note: you need the **Adobe Flash** plug-in on your web browser to display the world map. You can download a copy of Flash here: http://get.adobe.com/flashplayer.

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	
[j] 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.	

’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… [i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	

Dropped IPv4 Packet Log

Find by Date/Time Go No. of Lines 14 Go First Prev Next Last

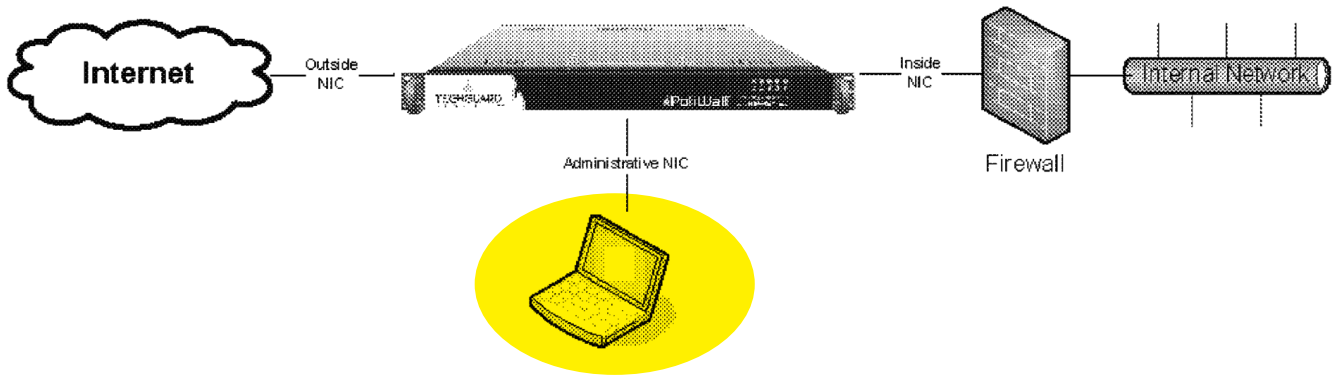
LINE NO.	DATE/TIME MS	SRC IP:PORT	DEST IP:PORT	PROTOCOL	FLAGS	DIRECTION	CAUSE	COUNTRY
339385	2010-08-24T14:32:03.984+0000	203.187.151.128:36941	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339386	2010-08-24T14:32:03.992+0000	192.150.24.152:35945	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339387	2010-08-24T14:32:03.994+0000	199.193.13.134:35949	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339388	2010-08-24T14:32:04.009+0000	144.29.164.122:35956	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339389	2010-08-24T14:32:04.046+0000	162.79.163.121:35974	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339390	2010-08-24T14:32:04.087+0000	131.151.72.166:36002	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339391	2010-08-24T14:32:04.089+0000	209.40.225.89:36004	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339392	2010-08-24T14:32:04.099+0000	167.254.182.15:36006	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339393	2010-08-24T14:32:04.101+0000	198.254.49.16:36008	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339394	2010-08-24T14:32:04.123+0000	44.239.250.75:36018	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339395	2010-08-24T14:32:04.124+0000	206.251.170.145:36020	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339396	2010-08-24T14:32:04.134+0000	64.140.191.93:36025	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339397	2010-08-24T14:32:04.173+0000	167.124.216.60:36052	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES
339398	2010-08-24T14:32:04.186+0000	74.7.109.127:36057	192.168.18.123:80	TCP	SYN	Inbound	country filter	UNITED STATES

The **Dropped IPv4 Packet Log** and the **Dropped IPv6 Packet Log** screens show you information on data packets blocked by the PoliWall.

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	✓
[j] 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.	

’722 Patent Analysis – PoliWall™

’722 Patent:	PoliWall™
1… [j] 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 following diagram shows the typical placement of the PoliWall in a network between the Internet border router and your firewall. 

PoliWall™ Invalidates the ’722 Patent, Claim 1

’722 Patent:	PoliWall™
1. [a] 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;	✓
[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;	✓
[c] 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;	✓
[d] 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;	✓
[e] 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;	✓
[f] 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	✓
[g] 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	✓
[h] 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	✓
[i] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	✓
[j] 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.	✓

Anue 5236 Net Tool Optimizer (NTO)

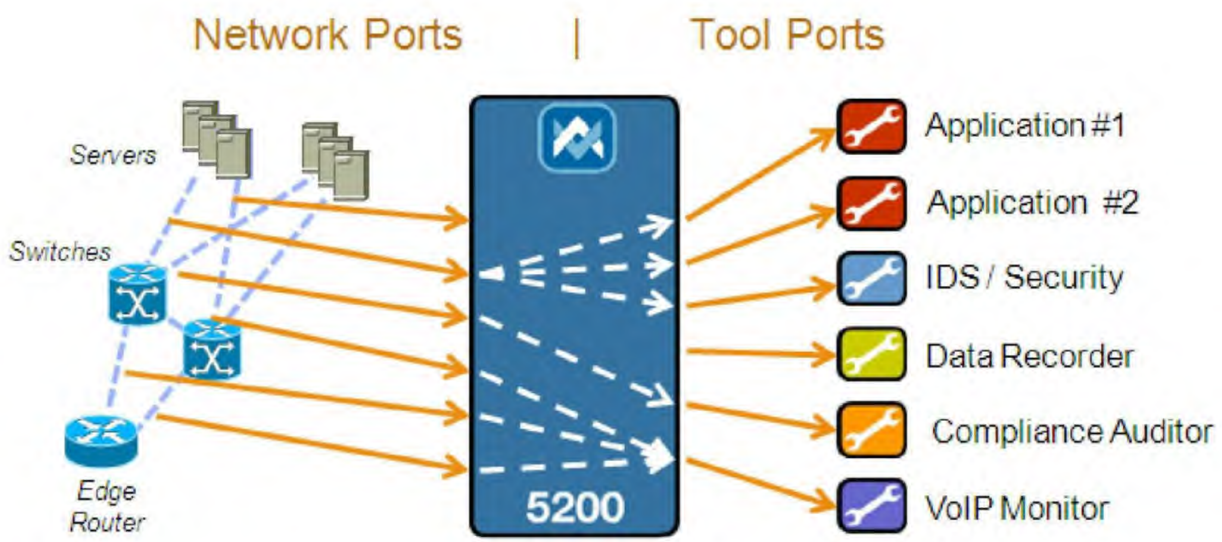
Anue NTO 5236 Invalidates the ’077 Patent Claims 7 and 13

NTO 5236 Invalidates the ’077 Patent Claim 7

’077 Patent:	NTO 5236
7. [a] 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:	
[b] 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; and	
[c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	
[d] 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; and	
[e] 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.	

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 329

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7. **[a]** 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:	 **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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 330

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7. **[a]** 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:	 **Figure 3 - Anue 5236 Net Tool Optimizer** **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.

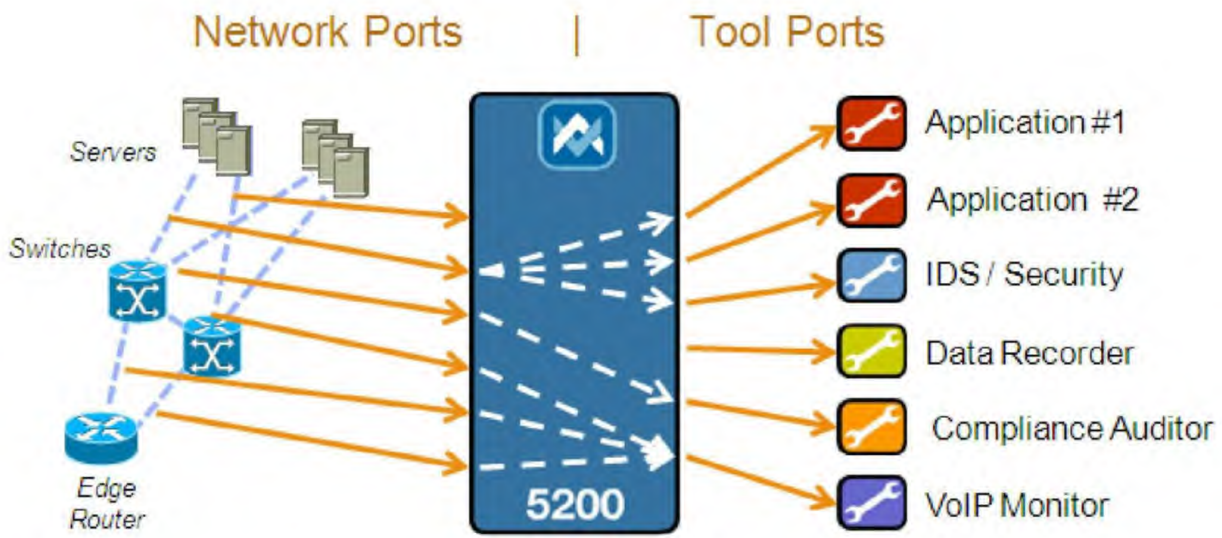
Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 331

NTO 5236 Invalidates the ’077 Patent Claim 7

’077 Patent:	NTO 5236
7. [a] 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:	✓
[b] 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; and	
[c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	
[d] 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; and	
[e] 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.	

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 332

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7… **[b]** 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; and	 **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.

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7… **[b]** 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; and	Ports designated through software as **Network Ports are used to connect TAP and SPAN ports to the Anue 5200**. Ports designated through software as **Tool Ports are used to connect tools such as data recorders and VoIP monitors to the Anue 5200**. The Net Tool Optimizer server runs on the 5200 chassis and the Control Panel client, a Java based graphical user interface (GUI), is provided so that the configuration and visualization of port mappings is easy and intuitive. Multiple users can manage the Net Tool Optimizer simultaneously and passwords and security capabilities can be assigned. The Anue 5200 server manages access to the configuration database. Users are warned when potential database conflicts exist and are allowed to decide if changes are saved to the database. Statistics are also provided to help manage tool utilization and optimization.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 334

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7… [b] 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; and	**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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 335

NTO 5236 Invalidates the ’077 Patent Claim 7

’077 Patent:	NTO 5236
7. **[a]** 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:	✓
[b] 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; and	✓
[c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	
[d] 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; and	
[e] 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.	

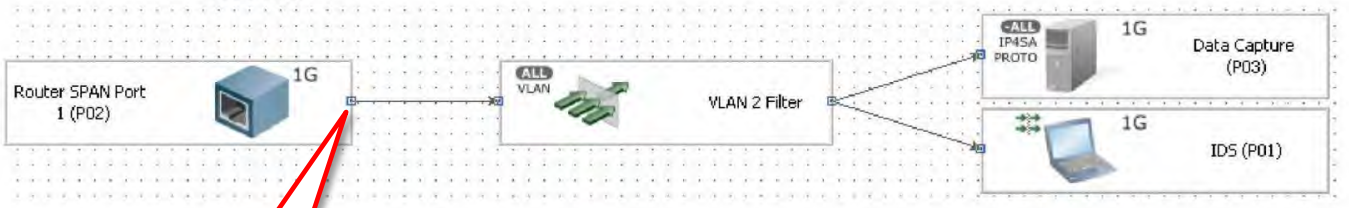
Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 336

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7… [c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	**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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 337

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7… **[c]** configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	**Result:**  **Figure 42 - SPAN Port Connected to 2 Tool Ports** **Ingress filter**

NTO 5236 Invalidates the ’077 Patent Claim 7

’077 Patent:	NTO 5236
7. **[a]** 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:	✓
[b] 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; and	✓
[c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	✓
[d] 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; and	
[e] 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.	

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 339

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7… [d] 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; and	**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.

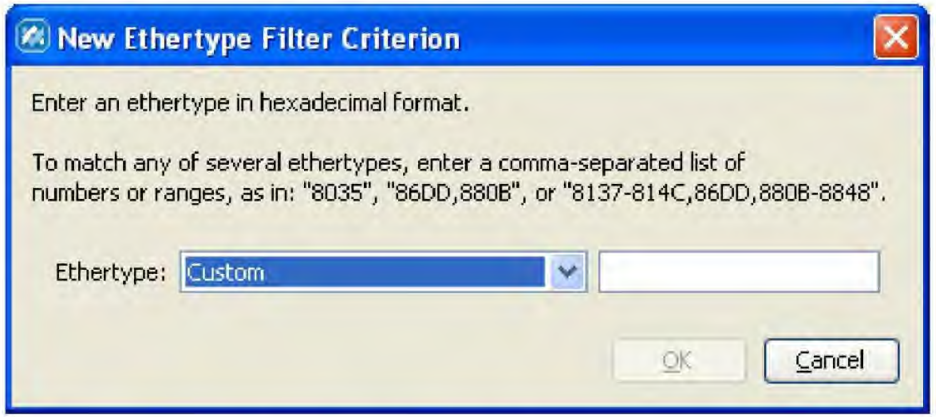
Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 340

NTO 5236 Invalidates the ’077 Patent Claim 7

’077 Patent:	NTO 5236
7. **[a]** 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:	✓
[b] 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; and	✓
[c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	✓
[d] 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; and	✓
[e] 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.	

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 341

’077 Patent Analysis – Anue Net Tool Optimizer (NTO) 5236

’077 Patent:	NTO 5236
7… [e] 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.	**VLAN ID:** Enter a single VLAN id (e.g. “100”), a comma-separated list of VLAN ids (e.g. “100,200” or a range of VLAN ids (e.g. “200-500”). A combination of all three types of entries can also be entered (e.g. “100-200,300,200-500”). **Priority:** Enter a 3 bit priority value. Specify “don’t care” bits using the letter “x” (e.g. “10x”). **Ethertype:** Select a well known Ethertype or define a custom value in hex. To match any of several Ethertypes, enter a comma-separated list of numbers or ranges. For example, “8035”, “86DD,880B” or “8137-814C,86DD,880B-8858”.  **Figure 65 - Ethertype Filter Criterion Window**

NTO 5236 Invalidates the ’077 Patent Claim 7

’077 Patent:	NTO 5236
7. **[a]** 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:	✓
[b] 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; and	✓
[c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	✓
[d] 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; and	✓
[e] 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.	✓

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 343

’077 Patent – Claims 7 and 13 Comparison

7. 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:	13. One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:
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; and	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; and
configure, each device of the plurality of devices, to:	configure, each device of the plurality of devices, to:
receive packets via a communication interface that does not have a network-layer address;	receive packets via a communication interface that does not have a network-layer address;
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; and	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; 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.	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.

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 344

NTO 5236 Invalidates the ’077 Patent Claim 13

’077 Patent:	NTO 5236
13. [a] One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:	✓
[b] 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; and	✓
[c] configure, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address;	✓
[d] 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; and	✓
[e] 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.	✓

Patent Owner, Centripetal Networks, Inc. - Ex. 2009, p. 345