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

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	No. 2:17-cv-00383 (HCM-LRL)
	)	
KEYSIGHT TECHNOLOGIES, INC., and IXIA,	)	
	)	
	)	
Defendants.	)	

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Centripetal Networks, Inc. ("Centripetal"), for its Complaint against Keysight Technologies, Inc. ("Keysight") and Ixia (collectively, "Defendants"), hereby alleges as follows:

THE PARTIES

1. Plaintiff Centripetal is a corporation organized under the laws of the state of Delaware with its principal place of business at 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171. Centripetal was founded with a strong focus on innovation and technology leadership that aligns to its core mission and purpose to protect networks from advanced threats. Centripetal has invented core-networking technologies that meet the scale of the cyber threat intelligence challenge. Centripetal maintains the largest threat intelligence partner ecosystem, providing community based solutions to defeat sophisticated cyberattacks. In recognition of its innovation and expertise, Centripetal has been awarded numerous patents enabling its key technological advances in the network security area.

2. Defendant Keysight is a Delaware corporation with its principal place of business

at 1400 Fountain Grove Parkway, Santa Rosa, California 95403. Keysight maintains a regular and established place of business in this District through a permanent physical facility located at 43130 Amberwood Plaza #200, Chantilly, VA 20152. Keysight maintains a group known as the "Ixia Solutions Group."

3. Defendant Ixia is a California corporation with its principal place of business at 26601 W. Agoura Rd, Calabasas, California 91302. Ixia maintains a regular and established place of business in this District through a permanent physical facility located at 1593 Spring Hill Road, Suite 530, Vienna, Virginia 22182. Keysight acquired Ixia on April 18, 2017, and operates Ixia as a division under the name "Ixia Solutions Group." On information and belief, Ixia is a wholly owned subsidiary of Keysight. On its website, Ixia states that "Ixia is now part of Keysight Technologies." *See, e.g.*, https://www.ixiacom.com. Keysight states on its website that Bethany Mayer, the President and CEO of Ixia before the acquisition, serves as a Vice President of Keysight and as President of Keysight's "Ixia Solutions Group." *See* https://www.ixiacom.com/company/leadership. Following the merger, Ixia's board of directors consists of Jeffrey Li, Vice President, Assistant General Counsel and Assistant Secretary at Keysight, and Jason Kary, Vice President, Treasurer & Investor Relations at Keysight. *See* Ixia 8-K, Item 5.02, April 18, 2017. Keysight's Senior Vice President Neil Dougherty serves as president of the Ixia subsidiary following the merger. *Id.*

4. Defendants regularly conduct and transact business in Virginia, throughout the United States, and within the Eastern District of Virginia, and as set forth below, have committed and continue to commit, tortious acts of patent infringement within and outside of Virginia and within the Eastern District of Virginia. Keysight maintains a regular and established place of business in this District through a permanent physical facility located at 43130 Amberwood

Plaza #200, Chantilly, VA 20152. Ixia maintains a regular and established place of business in this District through a permanent physical facility located at 1593 Spring Hill Road, Suite 530, Vienna, Virginia 22182. Further, the Defendants directly or indirectly use, distribute, market, sell, and/or offer to sell throughout the United States, including in this judicial district, various telecommunication products, including computing devices, associated equipment, and software.

5. Defendants' infringement of the asserted patents has been willful and deliberate because Defendants knew or were willfully blind to the asserted patents and their infringement of those patents but acted both with subjective bad faith and despite an objectively high likelihood that its acts would infringe the asserted patents. Centripetal notes on its website that its technology is protected by multiple patents, including the asserted patents: "Centripetal Networks has been awarded over 20 patents enabling unique technological advantages for our customers cyber security defenses." *See, e.g.*, https://www.centripetalnetworks.com/about.php. Defendants knew of this disclosure on Centripetal's website, yet acted with an objectively high likelihood that its acts would infringe. For example, employees from Anue Systems, Inc., a company Ixia acquired in 2012, visited Centripetal's website at least as early as 2014 and have continued to the present. Website tracking reports indicate that those employees regularly viewed Centripetal's web pages, including the specific pages explaining that Centripetal's technology was protected by numerous patents. For example, reports indicate that Scott Register, who was previously Sr. Director of Product Management for Ixia's Anue Net Tool Optimizer and is now Ixia's current Vice President of Product Management "leading the development of new Ixia products in the areas of Security, Virtualization and Cloud" regularly viewed Centripetal's web pages. *See, e.g.*, https://www.ixiacom.com/person/scott-register; Ixia Leadlander (Scot Register).pdf. Mr. Register has regularly promoted the accused products,

including the ThreatARMOR devices. *Id.* Centripetal also marks its products with its patents. Defendants thus knew or were willfully blind to Centripetal's technology and its patents. Further, on May 2, 2016, in an article written by Jon Oltsik in *Network World* titled "The Rise of Threat Intelligence Gateways," Mr. Oltsik detailed functions of threat intelligence gateways provided by a number of vendors, including Centripetal. Defendants use several quotes from Mr. Oltsik on their web sites, including, for example, at https://www.ixiacom.com/products/threatarmor. Moreover, Defendants have held webinars with Mr. Oltsik to promote their products. This further demonstrates that Defendants knew or were willfully blind to Centripetal's technology. Despite this knowledge and/or willful blindness, Defendants have acted with an objectively high likelihood of infringement.

JURISDICTION AND VENUE

6. This is an action for patent infringement arising under the patent laws of the United States, Title 35, United States Code. This Court has exclusive subject matter jurisdiction over this case for patent infringement under 28 U.S.C. § 1338.

7. This Court has personal jurisdiction over Defendants. Defendants have conducted and do conduct business within the State of Virginia. Keysight maintains a regular and established place of business in this District through a permanent physical facility located at 43130 Amberwood Plaza #200, Chantilly, VA 20152. Ixia maintains a regular and established place of business in this District through a permanent physical facility located at 1593 Spring Hill Road, Suite 530, Vienna, Virginia 22182. Defendants, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ship, distribute, offer for sale, sell, and advertise (including the provision of an interactive web page) their products and/or services in the United States, the State of Virginia, and the Eastern District of Virginia. Defendants,

directly and through subsidiaries or intermediaries (including distributors, retailers, and others), have purposefully and voluntarily placed one or more of their infringing products and/or services, as described below, into the stream of commerce with the expectation that they will be purchased and used by consumers in the Eastern District of Virginia. These infringing products and/or services have been and continue to be purchased and used by consumers in the Eastern District of Virginia. Defendants have committed acts of patent infringement within the State of Virginia and, more particularly, within the Eastern District of Virginia.

8. Venue is proper in the Eastern District of Virginia under 28 U.S.C. §§ 1391 and 1400(b). Defendants have transacted business in this District, and have directly committed acts of patent infringement in this District, and have a regular and established place of business in this District. Keysight maintains a regular and established place of business in this District through a permanent physical facility located at 43130 Amberwood Plaza #200, Chantilly, VA 20152. Ixia maintains a regular and established place of business in this District through a permanent physical facility located at 1593 Spring Hill Road, Suite 530, Vienna, Virginia 22182. Upon information and belief, Defendants employ a number of personnel in this District, including personnel involved in Defendants' infringement by at least through the testing, demonstration, use, offer for sale, and sale of the accused products and services within Virginia.

THE PATENTS IN SUIT

9. On February 16, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,264,370 ("the '370 patent"), entitled "Correlating Packets in Communications Networks." A true and correct copy of the '370 patent is attached hereto as Exhibit A.

10. On September 15, 2015, the United States Patent and Trademark Office duly and

legally issued U.S. Patent No. 9,137,205 ("the '205 patent"), entitled "Method and Systems for Protecting a Secured Network." A true and correct copy of the '205 patent is attached hereto as Exhibit B.

11. On January 31, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,560,077 ("the '077 patent"), entitled "Method and Systems for Protecting a Secured Network." A true and correct copy of the '077 patent is attached hereto as Exhibit C.

12. On August 9, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,413,722 ("the '722 patent"), entitled "Rule-Based Network-Threat Detection." A true and correct copy of the '722 patent is attached hereto as Exhibit D.

13. On February 7, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,565,213 ("the '213 patent"), entitled "Methods and Systems for Protecting a Secured Network." A true and correct copy of the '213 patent is attached hereto as Exhibit E.

14. On March 13, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,917,856 ("the '856 patent"), entitled "Rule-based Network-Threat Detection for Encrypted Communications." A true and correct copy of the '856 patent is attached hereto as Exhibit F.

15. Centripetal owns by assignment the entire right, title, and interest in and to the '370 patent, the '205 patent, the '077 patent, the '722 patent, the '213 patent, and the '856 patent (collectively, "the Asserted Patents").

16. All of the Asserted Patents are valid and enforceable.

17. Defendants have infringed and continue to infringe one or more claims of each of

the Asserted Patents by engaging in acts that constitute infringement under 35 U.S.C. § 271, including but not necessarily limited to making, using, selling, and/or offering for sale, in this district and elsewhere in the United States, and/or importing into this district and elsewhere in the United States, certain network security devices (collectively, "the Accused Products").

FIRST CAUSE OF ACTION
(Patent Infringement of the '370 Patent)

18. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

19. Defendants have infringed and continue to infringe, literally or under the doctrine of equivalents, the '370 patent by making, using, selling, offering for sale within the United States, and/or importing into the United States, products that are covered by one or more claims of the '370 patent. Such products include certain network security devices, including but not limited to the Ixia ThreatARMOR devices ("Accused '370 Products").

20. For example, Defendants have infringed, and continue to infringe, at least claim 22 of the '370 patent:

> 22. 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:
>
> provision a device in a communication link interfacing a network device and a first network with one or more rules configured to identify a plurality of packets received by the network device from a host located in the first network;
>
> provision a device in a communication link interfacing the network device and a second network with one or more rules configured to identify a plurality of packets transmitted by the network device to a host located in a second network;
>
> provision the device in the communication link interfacing the network device and the first network and the device in the communication link interfacing the network device and the second network with one or more rules specifying a set of network

addresses and configured to cause the system to log packets destined for one or more network addresses in the set of network addresses;

configure the device in the communication link interfacing the network device with the first network to:

identify the plurality of packets received by the network device;

generate a plurality of log entries corresponding to the plurality of packets received by the network device; and

communicate, to the system, the plurality of log entries corresponding to the plurality of packets received by the network device;

configure the device in the communication link interfacing the network device with the second network to:

identify the plurality of packets transmitted by the network device;

generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device; and

communicate, to the system, the plurality of log entries corresponding to the plurality of packets transmitted by the network device;

correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and

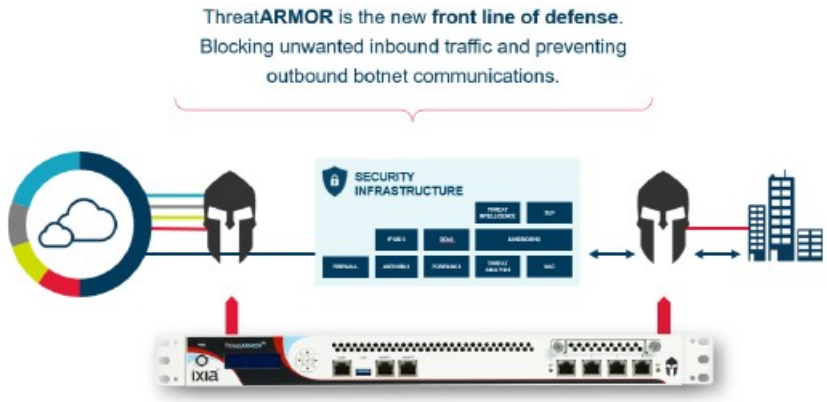
responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:

generate data identifying the host located in the first network; and

communicate, to a device located in the first network, the data identifying the host located in the first network.

21. The Accused '370 Products are "system[s] comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to . . . ." *See, e.g.*, Ixia ThreatARMOR Data Sheet, Doc. No. 915-3143-01-2161 Rev F ("ThreatARMOR Data Sheet"), at 1-2, attached hereto as Exhibit G. The Accused '370 Products

contain instructions to "provision a device in a communication link interfacing a network device and a first network with one or more rules configured to identify a plurality of packets received by the network device from a host located in the first network" and "provision a device in a communication link interfacing the network device and a second network with one or more rules configured to identify a plurality of packets transmitted by the network device to a host located in a second network and configured to cause the system to log packets destined for one or more network addresses in the set of network addresses":



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

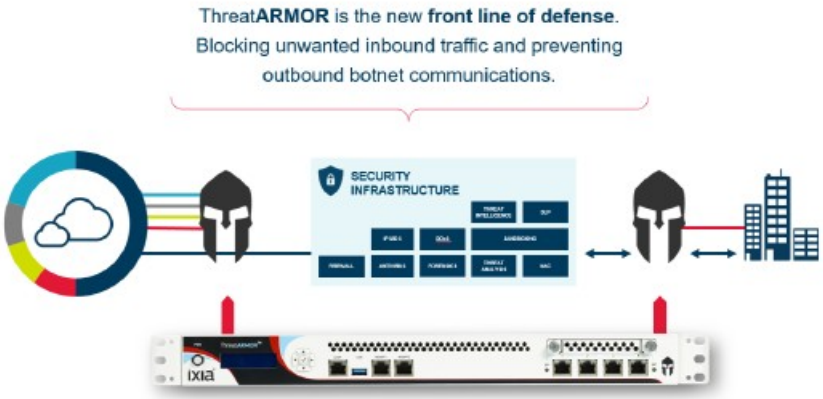
See Ixia Application and Threat Intelligence (ATI) Data Sheet, Doc. No. 915-6709-01 Rev D ("ATI Data Sheet"), at 3, attached hereto as Exhibit H. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Case Study, Financial Investment Firm Reduces Risk, Doc. No. 915-3591-01-5061 REV D ("Ixia Financial Case Study"), at 3-4, attached hereto as Exhibit I. For example, Defendants note that it "connected the first management port of the ThreatARMOR into their air-gapped management network and our other management port, designed to get 'Rap Sheet' updates, into a DMZ that has access to the Internet. The first management interface acquired an

IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard within minutes of racking the system." *Id.* at 3-4 (footnotes omitted). As Defendants explain, "Within one hour we began seeing 'Rap Sheets' describing network traffic events originated or destined to known bad IP addresses. The information gleaned by the rap sheet was very straight forward, classifying the remote IP address in varying categories such as hijacked, phishing, malware, etc." *Id.* at 4.

22. The Accused '370 Products contain instructions to "configure the device in the communication link interfacing the network device with the first network to: identify the plurality of packets received by the network device; generate a plurality of log entries corresponding to the plurality of packets received by the network device; and communicate, to the system, the plurality of log entries corresponding to the plurality of packets received by the network device." For example, Defendants note that it "connected the first management port of the ThreatARMOR into their air-gapped management network and our other management port, designed to get 'Rap Sheet' updates, into a DMZ that has access to the Internet. The first management interface acquired an IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard within minutes of racking the system." *See* Ixia Financial Case Study, at 3-4 (footnotes omitted). As Defendants explain, "Within one hour we began seeing 'Rap Sheets' describing network traffic events originated or destined to known bad IP addresses. The information gleaned by the rap sheet was very straight forward, classifying the remote IP address in varying categories such as hijacked, phishing, malware, etc." *Id.* at 4.

23. The Accused '370 Products contain instructions to "configure the device in the

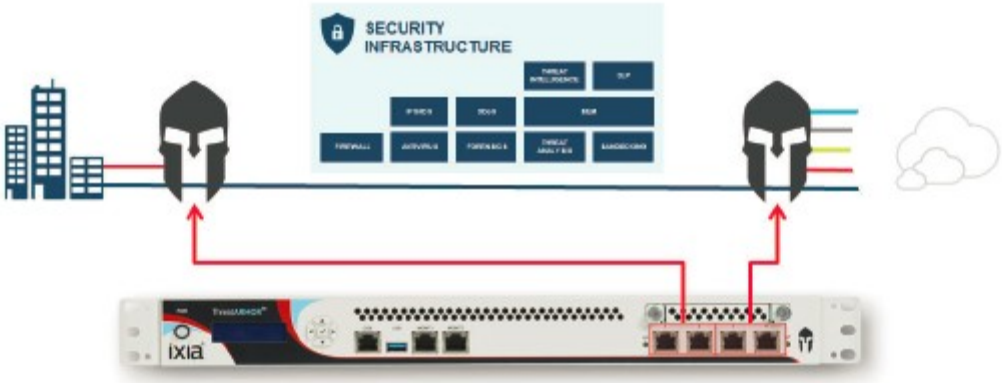
communication link interfacing the network device with the second network to: identify the plurality of packets transmitted by the network device; generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device; and communicate, to the system, the plurality of log entries corresponding to the plurality of packets transmitted by the network device." For example, Defendants note that it "connected the first management port of the ThreatARMOR into their air-gapped management network and our other management port, designed to get 'Rap Sheet' updates, into a DMZ that has access to the Internet. The first management interface acquired an IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard within minutes of racking the system." *See* Ixia Financial Case Study, at 3-4 (footnotes omitted). As Defendants explain, "Within one hour we began seeing 'Rap Sheets' describing network traffic events originated or destined to known bad IP addresses. The information gleaned by the rap sheet was very straight forward, classifying the remote IP address in varying categories such as hijacked, phishing, malware, etc." *Id.* at 4. The Accused '370 Products contain instructions to "correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device":



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet, at 3. Similarly:

When deployed in your security infrastructure, ThreatARMOR lowers your attack surface by blocking unwanted traffic from the Internet, and it blocks outbound connections to malicious sites from inside your network.



For example, if someone was to click on a phishing email, or an infected host tries to connect to an external botnet controller, ThreatARMOR will block those outbound connections.

See Reduce Your Network's Attack Surface, Doc. No. 915-6786-01 Rev. A ("ThreatARMOR Guide"), at 3, attached hereto as Exhibit J. Defendants explain that "The ThreatARMOR security appliance: [r]educes threats by blocking all traffic to and from known-bad sites and untrusted countries" and "[b]locks outbound Botnet communication from infected internal

systems." *See* ThreatARMOR Data Sheet at 2. Defendants further explain that "[o]ne event in particular was of high interest. An internal server IP address was flagged by ThreatARMOR as the target of an ongoing attack. This server was not meant to be directly accessible to the Internet. When the information gleaned from the Rap Sheet was correlated with information in the SIEM it was determined that a brute force SSH Login attempt had been going on for some time. The source of the attack was from a known hijacked IP address in Asia." Ixia Financial Case Study at 4.

24. Further, the Accused '370 Products, "responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device," contain instructions to "generate data identifying the host located in the first network; and communicate, to a device located in the first network, the data identifying the host located in the first network." For example, Defendants note that it "connected the first management port of the ThreatARMOR into their air-gapped management network and our other management port, designed to get 'Rap Sheet' updates, into a DMZ that has access to the Internet. The first management interface acquired an IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard within minutes of racking the system." *See* Ixia Financial Case Study, at 3-4 (footnotes omitted). As Defendants explain, "Within one hour we began seeing 'Rap Sheets' describing network traffic events originated or destined to known bad IP addresses. The information gleaned by the rap sheet was very straight forward, classifying the remote IP address in varying categories such as hijacked, phishing, malware, etc." *Id.* at 4. Defendants further explain that "[o]ne event in particular was of high interest. An internal server IP address was flagged by ThreatARMOR as the target of an ongoing attack. This server was not

meant to be directly accessible to the Internet. When the information gleaned from the Rap Sheet was correlated with information in the SIEM it was determined that a brute force SSH Login attempt had been going on for some time. The source of the attack was from a known hijacked IP address in Asia." *Id.* at 4.

25. In addition to directly infringing the '370 patent, Defendants have indirectly infringed and continue to indirectly infringe one or more claims of the '370 patent, including at least claim 22, by actively inducing others to directly infringe the '370 patent in violation of 35 U.S.C. § 271(b). For example, Defendants, with knowledge that the Accused '370 Products infringe the '370 patent at least as of the date of this Complaint and/or with willful blindness to the '370 patent, knowingly induced infringement of the '370 patent with specific intent to do so by their activities relating to the marketing, distribution, and/or sale of the Accused '370 Products to their purchasers, and by instructing and encouraging purchasers (including through product documentation) to operate and use those products in an infringing manner with knowledge that these actions would infringe the '370 patent. Further, as noted above, Defendants knew or were willfully blind to Centripetal's patents based on the interactions between Defendants and Centripetal. Moreover, as further detailed above, Defendants provide and market the Accused '370 Products to customers. Defendants further instruct and direct their customers on how to infringe the '370 patent by configuring the Accused '370 Products to be provisioned in a network and monitor and block outbound and inbound connections in a manner that infringes the '370 patent. *See* ThreatARMOR Data Sheet; Ixia Financial Case Study.

26. Defendants have contributed to direct infringement of the '370 patent, including by at least claim 22, by others by selling and/or offering for sale to their purchasers within the United States and/or importing into the United States products that are especially made and/or

adapted for infringing the ’370 patent and are not staple articles of commerce suitable for substantial noninfringing use and that have been sold to purchasers who infringe the ’370 patent, including but not limited to the Accused ’370 Products. Specifically, Defendants had knowledge at least as of the filing of this Complaint and/or were willfully blind to the fact that the Accused ’370 Products were specifically made and/or adapted for infringement of the ’370 patent and are not staple articles of commerce suitable for substantial noninfringing use.

27. Defendants’ infringement of the ‘370 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

28. Defendants have willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Defendants had knowledge of the Asserted Patents through various channels and despite their knowledge of Centripetal’s patent rights, engaged in egregious behavior warranting enhanced damages.

29. On or around July 2014, employees from Anue Systems, Inc., a company Ixia acquired in 2012, visited Centripetal’s website at least as early as 2014 and have continued to the present. *See, e.g.*, LeadLander Daily Report - Anue Systems 07-31-2014.pdf, attached hereto as Exhibit K; LeadLander Alert - Anue Systems 11-20-2014.pdf, attached hereto as Exhibit L; LeadLander Alert - Anue Systems 11-17-2015.pdf, attached hereto as Exhibit M. Website tracking reports indicate that those employees regularly viewed Centripetal’s web pages, including the specific pages explaining that Centripetal’s technology was protected by numerous patents. For example, reports indicate that Scott Register, who was previously Sr. Director of Product Management for Ixia’s Anue Net Tool Optimizer and is now Ixia’s current Vice President of Product Management “leading the development of new Ixia products in the areas of Security, Virtualization and Cloud” regularly viewed Centripetal’s web pages. *See, e.g.*,

https://www.ixiacom.com/person/scott-register, attached hereto as Exhibit N; Ixia Leadlander (Scot Register).pdf, attached hereto as Exhibit O. Mr. Register has regularly promoted the Accused Products, including the ThreatARMOR devices. *Id.*

30. Further, on May 2, 2016, in an article written by Jon Oltsik in *Network World* titled "The Rise of Threat Intelligence Gateways," Mr. Oltsik detailed functions of threat intelligence gateways provided by a number of vendors, including Centripetal. *See* J. Ostik, "The rise of threat intelligence gateways," available at https://www.csoonline.com/article/3064299/security/the-rise-of-threat-intelligence-gateways.html, attached hereto as Exhibit P. Defendants use several quotes from Mr. Oltsik on their web sites, including, for example, at https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T. Moreover, Defendants have held webinars with Mr. Oltsik to promote their products.

31. Defendants thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents.

32. Defendants' infringement of the '370 Patent is egregious. Centripetal is informed and believes that Defendants have been aware of Centripetal's products which are marked with its patents. For example, Centripetal builds and sells RuleGATE 2000, a product which is marked with at least the '722 Patent, '370 Patent, '205 Patent, the '213 Patent, and the '077 Patent. Despite their knowledge of Centripetal and its patents, Centripetal is informed and believes that Defendant's deliberately copied Centripetal's patented technology, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000, which Defendants implemented into their products and services. The blatant copying of Centripetal's patented technology is egregious behavior warranting a finding of

willful infringement and enhanced damages.

33. This further demonstrates that Defendants knew or, in the alternative, was willfully blind to Centripetal's Asserted Patents. Despite this knowledge and/or willful blindness, Defendants have acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

34. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '370 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '370 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '370 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

SECOND CAUSE OF ACTION
(Patent Infringement of the '205 Patent)

35. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

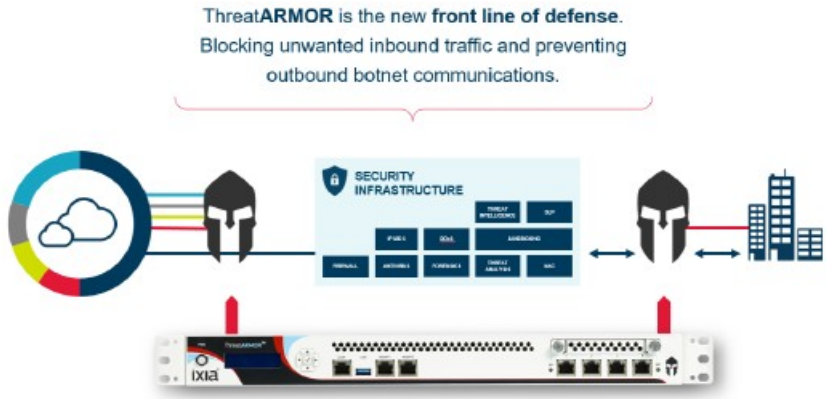
36. Defendants have infringed and continue to infringe, literally or under the doctrine of equivalents, the '205 patent by making, using, selling, offering for sale within the United States, and/or importing into the United States, products that are covered by one or more claims of the '205 patent. Such products include certain network security devices, including but not limited to the Ixia ThreatARMOR devices in conjunction with Ixia's Application and Threat Intelligence servers, including when used with Ixia's Vision ONE devices ("Accused '205 Products").

37. For example, Defendants have infringed, and continue to infringe, at least claim

91 of the ’205 patent:

> 91. A method, comprising:
>
> communicating, by a security policy management server and to a packet security gateway located at a first boundary of a network protected by the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary;
>
> communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary;
>
> performing, by the packet security gateway located at the first boundary, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary, wherein performing the at least one of the multiple packet transformation functions specified by the first dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the first boundary; and
>
> performing, by the packet security gateway located at the second boundary, at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary, wherein performing the at least one of the multiple packet transformation functions specified by the second dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the second boundary.

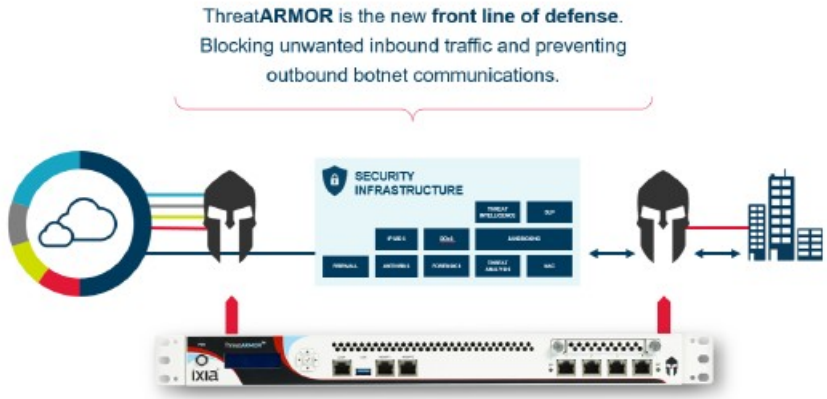
38. Defendants practice “[a] method, comprising: communicating, by a security policy management server and to a packet security gateway located at a first boundary of a network protected by the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary”:



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet, at 3. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Financial Case Study, at 3-4. For example, Defendants note that they "connected the first management port of the ThreatARMOR into their air-gapped management network and our other management port, designed to get 'Rap Sheet' updates, into a DMZ that has access to the Internet. The first management interface acquired an IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard within minutes of racking the system." *Id.* at 3-4 (footnotes omitted). Ixia's "ThreatARMOR devices automatically download updates from the ATI Research Center as frequently as every five minutes, giving you the most up-to-date list of known bad actors." *Id.* at 3.

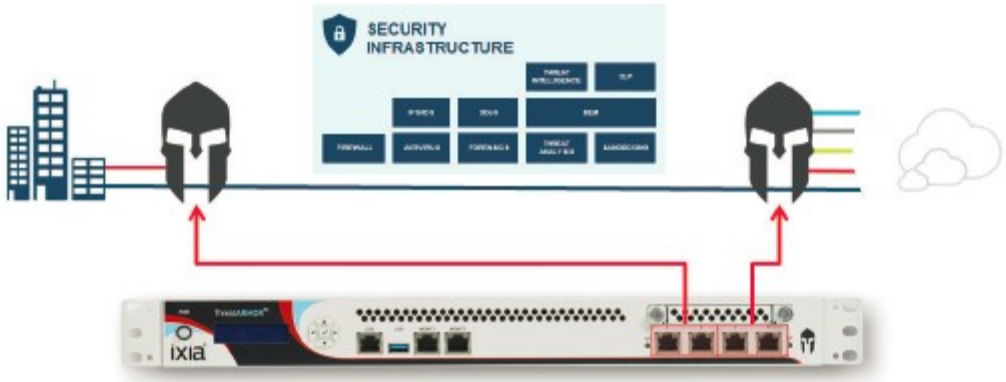
39. Defendants practice "communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary":



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet, at 3. Similarly:

When deployed in your security infrastructure, ThreatARMOR lowers your attack surface by blocking unwanted traffic from the Internet, and it blocks outbound connections to malicious sites from inside your network.

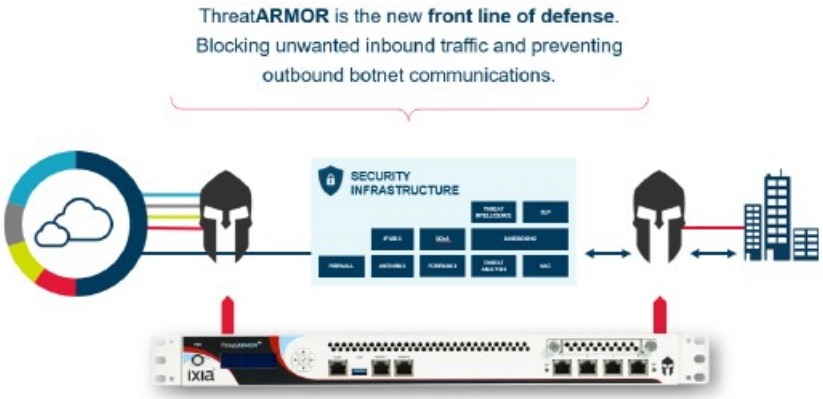


For example, if someone was to click on a phishing email, or an infected host tries to connect to an external botnet controller, ThreatARMOR will block those outbound connections.

See ThreatARMOR Guide at 3. Defendants explain that "The ThreatARMOR security appliance: [r]educes threats by blocking all traffic to and from known-bad sites and untrusted countries" and "[b]locks outbound Botnet communication from infected internal systems." *See*

ThreatARMOR Data Sheet at 2. Defendants further explain that "[o]ne event in particular was of high interest. An internal server IP address was flagged by ThreatARMOR as the target of an ongoing attack. This server was not meant to be directly accessible to the Internet. When the information gleaned from the Rap Sheet was correlated with information in the SIEM it was determined that a brute force SSH Login attempt had been going on for some time. The source of the attack was from a known hijacked IP address in Asia." Ixia Financial Case Study at 4. Ixia's "ThreatARMOR devices automatically download updates from the ATI Research Center as frequently as every five minutes, giving you the most up-to-date list of known bad actors." *Id.* at 3.

40. Defendants practice "performing, by the packet security gateway located at the first boundary, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary, wherein performing the at least one of the multiple packet transformation functions specified by the first dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the first boundary":

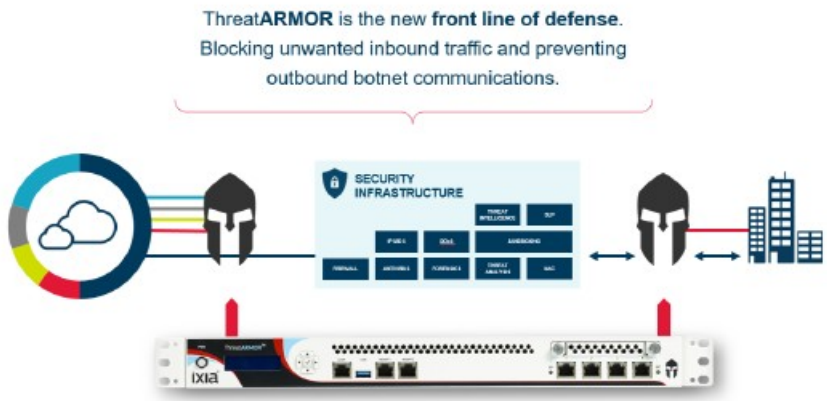


A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet at 3. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Financial Case Study, at 3. Defendants further explain that "[a]fter confidence was gained in the ThreatARMOR solution, the decision was made by the financial institution's security team to place our solution inline in 'blocking mode' in front of their NGFW. After the adjustment was made, we saw roughly 60,000 connections blocked in a single week, where the security events originated from all over the globe." *Id.* at 4-5. Defendants explain that "The ThreatARMOR security appliance: [r]educes threats by blocking all traffic to and from known-bad sites and untrusted countries" and "[b]locks outbound Botnet communication from infected internal systems." *See* ThreatARMOR Data Sheet at 2.

41. Defendants practice "performing, by the packet security gateway located at the second boundary, at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary, wherein performing the at least one of the multiple packet transformation functions

specified by the second dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the second boundary":



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet at 3. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Financial Case Study, at 3. Defendants further explain that "[a]fter confidence was gained in the ThreatARMOR solution, the decision was made by the financial institution's security team to place our solution inline in 'blocking mode' in front of their NGFW. After the adjustment was made, we saw roughly 60,000 connections blocked in a single week, where the security events originated from all over the globe." *Id.* at 4-5. Defendants explain that "The ThreatARMOR security appliance: [r]educes threats by blocking all traffic to and from known-bad sites and untrusted countries" and "[b]locks outbound Botnet communication from infected internal systems." *See* ThreatARMOR Data Sheet at 2.

42. In addition to directly infringing the '205 patent, Defendants have indirectly infringed and continue to indirectly infringe one or more claims of the '205 patent, including at

least claim 91, by actively inducing others to directly infringe the ’205 patent in violation of 35 U.S.C. § 271(b). For example, Defendants, with knowledge that the Accused ’205 Products infringe the ’205 patent at least as of the date of this Complaint and/or with willful blindness to the ’205 patent, knowingly induced infringement of the ’205 patent with specific intent to do so by their activities relating to the marketing, distribution, and/or sale of the Accused ’205 Products to their purchasers, and by instructing and encouraging purchasers (including through product documentation) to operate and use those products in an infringing manner with knowledge that these actions would infringe the ’205 patent. Further, as noted above, Defendants knew or were willfully blind to Centripetal’s patents based on the interactions between Defendants and Centripetal. Moreover, and as further detailed above, Defendants provide and market the Accused ’205 Products to customers. Defendants further instruct and direct their customers on how to infringe the ’205 patent by configuring the Accused ’205 Products to be provisioned in a network and monitor and block outbound and inbound connections in a manner that infringes the ’205 patent. *See* ThreatARMOR Data Sheet; Ixia Financial Case Study.

43. Defendants have contributed to direct infringement of the ’205 patent, including at least claim 91, by others by selling and/or offering for sale to their purchasers within the United States and/or importing into the United States products that are especially made and/or adapted for infringing the ’205 patent and are not staple articles of commerce suitable for substantial noninfringing use and that have been sold to purchasers who infringe the ’205 patent, including but not limited to the Accused ’205 Products. Specifically, Defendants had knowledge at least as of the filing of this Complaint and/or were willfully blind to the fact that the Accused ’205 Products were specifically made and/or adapted for infringement of the ’205 patent and are

not staple articles of commerce suitable for substantial noninfringing use.

44. Defendants' infringement of the '205 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

45. Defendants have willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Defendants had knowledge of the Asserted Patents through various channels and despite their knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

46. On or around July 2014, employees from Anue Systems, Inc., a company Ixia acquired in 2012, visited Centripetal's website at least as early as 2014 and have continued to the present. *See, e.g.*, LeadLander Daily Report - Anue Systems 07-31-2014.pdf, attached hereto as Exhibit K; LeadLander Alert - Anue Systems 11-20-2014.pdf, attached hereto as Exhibit L; LeadLander Alert - Anue Systems 11-17-2015.pdf, attached hereto as Exhibit M. Website tracking reports indicate that those employees regularly viewed Centripetal's web pages, including the specific pages explaining that Centripetal's technology was protected by numerous patents. For example, reports indicate that Scott Register, who was previously Sr. Director of Product Management for Ixia's Anue Net Tool Optimizer and is now Ixia's current Vice President of Product Management "leading the development of new Ixia products in the areas of Security, Virtualization and Cloud" regularly viewed Centripetal's web pages. *See, e.g.*, https://www.ixiacom.com/person/scott-register, attached hereto as Exhibit N; Ixia Leadlander (Scot Register).pdf, attached hereto as Exhibit O. Mr. Register has regularly promoted the Accused Products, including the ThreatARMOR devices. *Id.*

47. Further, on May 2, 2016, in an article written by Jon Oltsik in *Network World* titled "The Rise of Threat Intelligence Gateways," Mr. Oltsik detailed functions of threat

intelligence gateways provided by a number of vendors, including Centripetal. *See* J. Ostik, "The rise of threat intelligence gateways," available at https://www.csoonline.com/article/3064299/security/the-rise-of-threat-intelligence-gateways.html, attached hereto as Exhibit P. Defendants use several quotes from Mr. Oltsik on their web sites, including, for example, at https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T. Moreover, Defendants have held webinars with Mr. Oltsik to promote their products.

48. Defendants thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents.

49. Defendants' infringement of the '205 Patent is egregious. Centripetal is informed and believes that Defendants have been aware of Centripetal's products which are marked with its patents. For example, Centripetal builds and sells RuleGATE 2000, a product which is marked with at least the '722 Patent, '370 Patent, '205 Patent, the '213 Patent, and the '077 Patent. Despite their knowledge of Centripetal and its patents, Centripetal is informed and believes that Defendant's deliberately copied Centripetal's patented technology, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000, which Defendants implemented into their products and services. The blatant copying of Centripetal's patented technology is egregious behavior warranting a finding of willful infringement and enhanced damages.

50. This further demonstrates that Defendants knew or, in the alternative, was willfully blind to Centripetal's Asserted Patents. Despite this knowledge and/or willful blindness, Defendants have acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

51. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '205 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '205 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '205 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

THIRD CAUSE OF ACTION
(Patent Infringement of the '077 Patent)

52. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

53. Defendants have infringed and continue to infringe, literally or under the doctrine of equivalents, the '077 patent by making, using, selling, offering for sale within the United States, and/or importing into the United States, products that are covered by one or more claims of the '077 patent. Such products include certain network security devices, including but not limited to the Ixia ThreatARMOR, when used alone or with Ixia's Vision ONE devices ("Accused '077 Products").

54. For example, Defendants have infringed, and continue to infringe, at least claim 1 of the '077 patent:

1. A method comprising:

provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located; and

configuring, each device of the plurality of devices, to:

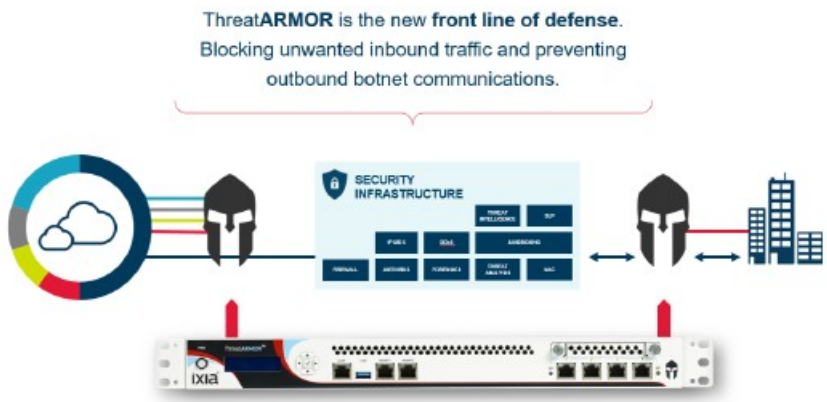
receive packets via a communication interface that does not have a

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

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.

55. Defendants practice "[a] method comprising: provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located":



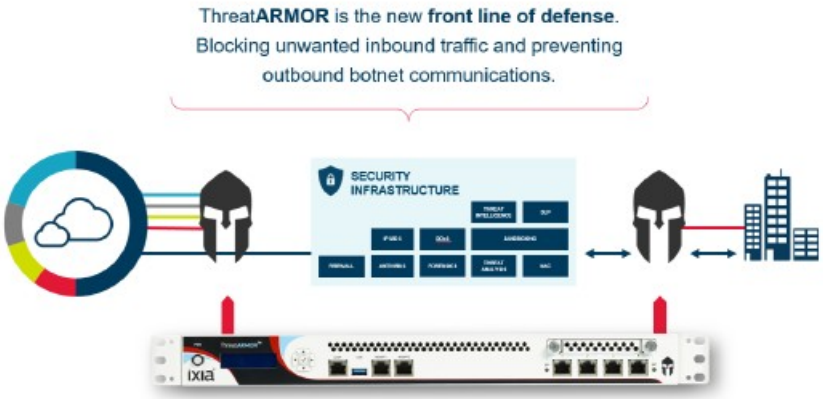
A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet at 3. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Financial Case Study, at 3. Further, when Ixia's Vision ONE is used, "Ixia's Vision ONE network packet broker (NPB) enables you to filter and visualize not only Level 2-4 traffic, but also Layer 7 application traffic, so that suspicious applications can be tagged and watched. This provides security advantages as

users can quickly spot rogue applications or unusual activity, including traffic or packets coming or going from unauthorized geographies, or questionable file transfer protocol (FTP) transfers conducted on sensitive data in the middle of the night." *See* https://www.ixiacom.com/products/vision-one, attached hereto as Exhibit Q.

56. Defendants practice "configuring, each device of the plurality of devices, to: receive packets via a communication interface that does not have a network-layer address." For example, Defendants note that they "connected the first management port of the ThreatARMOR into their air-gapped management network and our other management port, designed to get 'Rap Sheet' updates, into a DMZ that has access to the Internet. The first management interface acquired an IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard within minutes of racking the system." Ixia Financial Case Study, at 3-4 (footnotes omitted). Further, "On average, the tapped port from the NTO fed between 500Mbps and 750Mbps into the ThreatARMOR to be examined in 'Reporting Mode.'" *Id.* at 4. "[a]fter confidence was gained in the ThreatARMOR solution, the decision was made by the financial institution's security team to place our solution inline in 'blocking mode' in front of their NGFW. After the adjustment was made, we saw roughly 60,000 connections blocked in a single week, where the security events originated from all over the globe." *Id.* at 4-5.

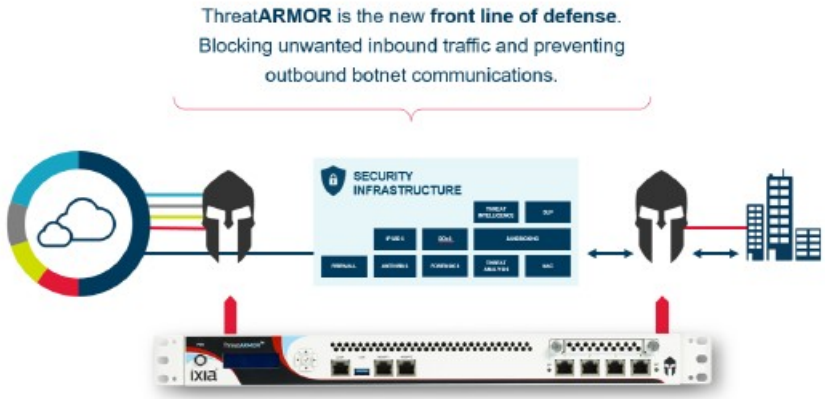
57. Defendants further configure each device of the plurality of devices to, "responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets":



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet at 3. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Financial Case Study, at 3. Defendants further explain that "[a]fter confidence was gained in the ThreatARMOR solution, the decision was made by the financial institution's security team to place our solution inline in 'blocking mode' in front of their NGFW. After the adjustment was made, we saw roughly 60,000 connections blocked in a single week, where the security events originated from all over the globe." Ixia Financial Case Study, at 4-5.

58. Defendants further configure each device of the plurality of devices to "modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device":



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet at 3. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Financial Case Study, at 3. Defendants further explain that "[a]fter confidence was gained in the ThreatARMOR solution, the decision was made by the financial institution's security team to place our solution inline in 'blocking mode' in front of their NGFW. After the adjustment was made, we saw roughly 60,000 connections blocked in a single week, where the security events originated from all over the globe." Ixia Financial Case Study, at 4-5. Further, ThreatARMOR uses "Ethernet interfaces with built-in bypass modes [that] ensure network availability on both the 1GbE copper and 10GbE fiber interfaces. ThreatARMOR Data Sheet at 1.

59. In addition to directly infringing the '077 patent, Defendants have indirectly infringed and continue to indirectly infringe one or more claims of the '077 patent, including at least claim 22, by actively inducing others to directly infringe the '077 patent in violation of 35 U.S.C. § 271(b). For example, Defendants, with knowledge that the Accused '077 Products infringe the '077 patent at least as of the date of this Complaint and/or with willful blindness to the '077 patent, knowingly induced infringement of the '077 patent with specific intent to do so

by their activities relating to the marketing, distribution, and/or sale of the Accused ’077 Products to their purchasers, and by instructing and encouraging purchasers (including through product documentation) to operate and use those products in an infringing manner with knowledge that these actions would infringe the ’077 patent. Further, as noted above, Defendants knew or were willfully blind to Centripetal’s patents based on the interactions between Defendants and Centripetal. Moreover, and as further detailed above, Defendants provide and market the Accused ’077 Products to customers. Defendants further instruct and direct their customers on how to infringe the ’077 patent by configuring the Accused ’077 Products to be provisioned in a network and monitor and block outbound and inbound connections in a manner that infringes the ’077 patent. *See* ThreatARMOR Data Sheet; Ixia Financial Case Study.

60. Defendants have contributed to direct infringement of the ’077 patent, including by at least claim 22, by others by selling and/or offering for sale to their purchasers within the United States and/or importing into the United States products that are especially made and/or adapted for infringing the ’077 patent and are not staple articles of commerce suitable for substantial noninfringing use and that have been sold to purchasers who infringe the ’077 patent, including but not limited to the Accused ’077 Products. Specifically, Defendants had knowledge at least as of the filing of this Complaint and/or was willfully blind to the fact that the Accused ’077 Products were specifically made and/or adapted for infringement of the ’077 patent and are not staple articles of commerce suitable for substantial noninfringing use.

61. Defendants’ infringement of the ‘077 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

62. Defendants have willfully infringed each of the Asserted Patents. Centripetal is

informed and believes that Defendants had knowledge of the Asserted Patents through various channels and despite their knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

63. On or around July 2014, employees from Anue Systems, Inc., a company Ixia acquired in 2012, visited Centripetal's website at least as early as 2014 and have continued to the present. *See, e.g.*, LeadLander Daily Report - Anue Systems 07-31-2014.pdf, attached hereto as Exhibit K; LeadLander Alert - Anue Systems 11-20-2014.pdf, attached hereto as Exhibit L; LeadLander Alert - Anue Systems 11-17-2015.pdf, attached hereto as Exhibit M. Website tracking reports indicate that those employees regularly viewed Centripetal's web pages, including the specific pages explaining that Centripetal's technology was protected by numerous patents. For example, reports indicate that Scott Register, who was previously Sr. Director of Product Management for Ixia's Anue Net Tool Optimizer and is now Ixia's current Vice President of Product Management "leading the development of new Ixia products in the areas of Security, Virtualization and Cloud" regularly viewed Centripetal's web pages. *See, e.g.*, https://www.ixiacom.com/person/scott-register, attached hereto as Exhibit N; Ixia Leadlander (Scot Register).pdf, attached hereto as Exhibit O. Mr. Register has regularly promoted the Accused Products, including the ThreatARMOR devices. *Id.*

64. Further, on May 2, 2016, in an article written by Jon Oltsik in *Network World* titled "The Rise of Threat Intelligence Gateways," Mr. Oltsik detailed functions of threat intelligence gateways provided by a number of vendors, including Centripetal. *See* J. Ostik, "The rise of threat intelligence gateways," available at https://www.csoonline.com/article/3064299/security/the-rise-of-threat-intelligence-gateways.html, attached hereto as Exhibit P. Defendants use several quotes from Mr. Oltsik on

their web sites, including, for example, at https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T. Moreover, Defendants have held webinars with Mr. Oltsik to promote their products.

65. Defendants thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents.

66. Defendants' infringement of the '077 Patent is egregious. Centripetal is informed and believes that Defendants have been aware of Centripetal's products which are marked with its patents. For example, Centripetal builds and sells RuleGATE 2000, a product which is marked with at least the '722 Patent, '370 Patent, '205 Patent, the '213 Patent, and the '077 Patent. Despite their knowledge of Centripetal and its patents, Centripetal is informed and believes that Defendant's deliberately copied Centripetal's patented technology, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000, which Defendants implemented into their products and services. The blatant copying of Centripetal's patented technology is egregious behavior warranting a finding of willful infringement and enhanced damages.

67. This further demonstrates that Defendants knew or, in the alternative, was willfully blind to Centripetal's Asserted Patents. Despite this knowledge and/or willful blindness, Defendants have acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

68. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '077 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '077 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately,

and egregiously engage in acts of infringement of the '077 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

FOURTH CAUSE OF ACTION
(Patent Infringement of the '722 Patent)

69. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

70. Defendants have infringed and continue to infringe, literally or under the doctrine of equivalents, the '722 patent by making, using, selling, offering for sale within the United States, and/or importing into the United States, products that are covered by one or more claims of the '722 patent. Such products include certain network security devices, including but not limited to the Ixia ThreatARMOR devices in conjunction with Ixia's Application and Threat Intelligence servers, including when used with Ixia's Vision ONE devices ("Accused '722 Products").

71. For example, Defendants have infringed, and continue to infringe, at least claim 1 of the '722 patent:

1. 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;

receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;

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;

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

causing, 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;

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

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

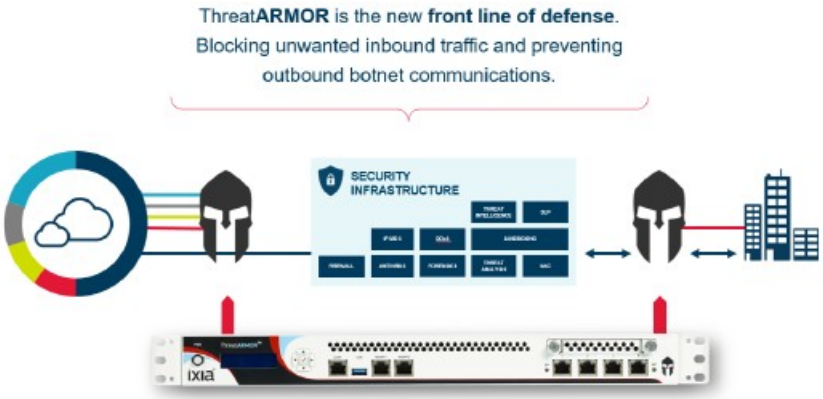
responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria:

preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;

communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and

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.

72. Defendants practice "[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":



A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound load on your firewall and SIEM from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

See ATI Data Sheet at 3. Further, "ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses." *See* Ixia Financial Case Study at 3-4. The Accused '722 Products perform the step of "receiving, by the packet- filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet." *See* ATI Data Sheet at 3.

73. The Accused '722 Products, "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," perform the step of "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." For example, "because all the IP addresses on the blocked list are updated daily, the handful of IP addresses that do revert to being benign are quickly re-allocated to the whitelist, but with a full 'rap sheet' on their history." Ixia, *'Instant protection' with a 'simple deployment' – ThreatARMOR earns five-star review*, available at

https://www.ixiacom.com/company/blog/'instant-protection'-'simple-deployment'---- threatarmor-earns-five-star-review, attached hereto as Exhibit R. Further, Ixia's Vision ONE devices "enable[] you to filter and visualize not only Level 2-4 traffic, but also Layer 7 application traffic, so that suspicious applications can be tagged and watched. This provides security advantages as users can quickly spot rogue applications or unusual activity, including traffic or packets coming or going from unauthorized geographies, or questionable file transfer protocol (FTP) transfers conducted on sensitive data in the middle of the night." *See* https://www.ixiacom.com/products/vision-one, attached hereto as Exhibit Q. Further:

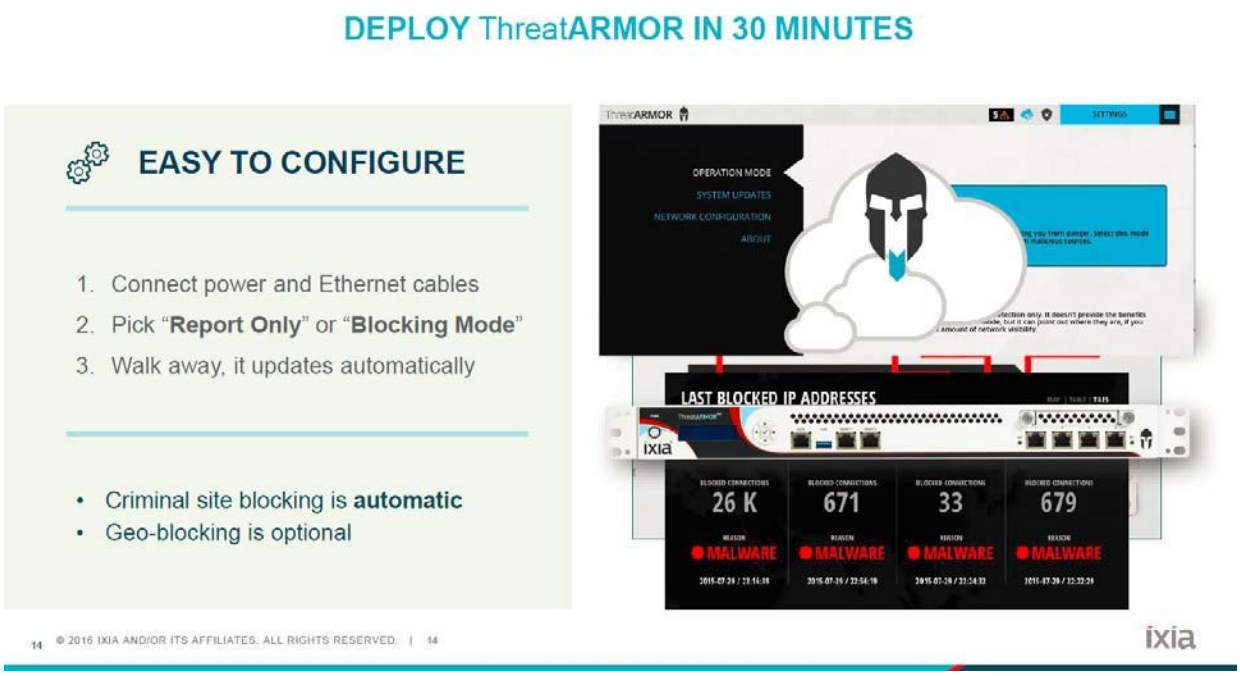
- Extensive packet filtering capabilities, including:
  - Layer 2: MAC, VLAN, MPLS, or Ethertype
  - Layer 3: IPv4 or IPv6, source / dest / session, DSCP, IP Protocol
  - Layer 4: Port Number, TCP Control

See Vision ONE Data Sheet, Doc. No.: 915-6691-01 Rev A, at 2, attached hereto as Exhibit S.

74. Further, the Accused '722 Products perform the step of "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" and "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":

See https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T.

75. The Accused '722 Products perform the step of "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 "responsive to receiving the instruction," the Accused '722 Products perform the step of "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":



See Front Line Security ThreatARMOR, available at https://www.youtube.com/watch?v=TYdlwW2yeb8&t=366s.

76. Further, "responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria," the Accused '722 Products perform the step of "preventing, by the packet-filtering device, the second packet from continuing toward a

destination of the second packet." For example, Defendants note that it "connected the first management port of the ThreatARMOR into their air-gapped management network and our other management port, designed to get 'Rap Sheet' updates, into a DMZ that has access to the Internet. The first management interface acquired an IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard within minutes of racking the system." Ixia Financial Case Study at 3-4 (footnotes omitted). As Defendants explain, "Within one hour we began seeing 'Rap Sheets' describing network traffic events originated or destined to known bad IP addresses. The information gleaned by the rap sheet was very straight forward, classifying the remote IP address in varying categories such as hijacked, phishing, malware, etc." *Id.* at 4.

77. Further, the Accused '722 Products perform the step of "communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet" and "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":

See https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T.

78. In addition to directly infringing the ’722 patent, Defendants have indirectly infringed and continue to indirectly infringe one or more claims of the ’722 patent, including at least claim 1, by actively inducing others to directly infringe the ’722 patent in violation of 35 U.S.C. § 271(b). For example, Defendants, with knowledge that the Accused ’722 Products infringe the ’722 patent at least as of the date of this Complaint and/or with willful blindness to the ’722 patent, knowingly induced infringement of the ’722 patent with specific intent to do so by their activities relating to the marketing, distribution, and/or sale of the Accused ’722 Products to their purchasers, and by instructing and encouraging purchasers (including through product documentation) to operate and use those products in an infringing manner with knowledge that these actions would infringe the ’722 patent. Further, as noted above, Defendants knew or were willfully blind to Centripetal’s patents based on the interactions

between Defendants and Centripetal. Moreover, and as further detailed above, Defendants provide and market the Accused '722 Products to customers. Defendants further instruct and direct their customers on how to infringe the '722 patent by configuring the Accused '722 Products to be provisioned in a network and monitor and block outbound and inbound connections in a manner that infringes the '722 patent. *See* ThreatARMOR Data Sheet; Ixia Financial Case Study.

79. Defendants have contributed to direct infringement of the '722 patent, including by at least claim 22, by others by selling and/or offering for sale to their purchasers within the United States and/or importing into the United States products that are especially made and/or adapted for infringing the '722 patent and are not staple articles of commerce suitable for substantial noninfringing use and that have been sold to purchasers who infringe the '722 patent, including but not limited to the Accused '722 Products. Specifically, Defendants had knowledge at least as of the filing of this Complaint and/or was willfully blind to the fact that the Accused '722 Products were specifically made and/or adapted for infringement of the '722 patent and are not staple articles of commerce suitable for substantial noninfringing use.

80. Defendants' infringement of the '722 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

81. Defendants have willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Defendants had knowledge of the Asserted Patents through various channels and despite their knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

82. On or around July 2014, employees from Anue Systems, Inc., a company Ixia acquired in 2012, visited Centripetal's website at least as early as 2014 and have continued to the

present. *See, e.g.*, LeadLander Daily Report - Anue Systems 07-31-2014.pdf, attached hereto as Exhibit K; LeadLander Alert - Anue Systems 11-20-2014.pdf, attached hereto as Exhibit L; LeadLander Alert - Anue Systems 11-17-2015.pdf, attached hereto as Exhibit M. Website tracking reports indicate that those employees regularly viewed Centripetal's web pages, including the specific pages explaining that Centripetal's technology was protected by numerous patents. For example, reports indicate that Scott Register, who was previously Sr. Director of Product Management for Ixia's Anue Net Tool Optimizer and is now Ixia's current Vice President of Product Management "leading the development of new Ixia products in the areas of Security, Virtualization and Cloud" regularly viewed Centripetal's web pages. *See, e.g.*, https://www.ixiacom.com/person/scott-register, attached hereto as Exhibit N; Ixia Leadlander (Scot Register).pdf, attached hereto as Exhibit O. Mr. Register has regularly promoted the Accused Products, including the ThreatARMOR devices. *Id.*

83. Further, on May 2, 2016, in an article written by Jon Oltsik in *Network World* titled "The Rise of Threat Intelligence Gateways," Mr. Oltsik detailed functions of threat intelligence gateways provided by a number of vendors, including Centripetal. *See* J. Ostik, "The rise of threat intelligence gateways," available at https://www.csoonline.com/article/3064299/security/the-rise-of-threat-intelligence-gateways.html, attached hereto as Exhibit P. Defendants use several quotes from Mr. Oltsik on their web sites, including, for example, at https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T. Moreover, Defendants have held webinars with Mr. Oltsik to promote their products.

84. Defendants thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents.

85. Defendants' infringement of the '722 Patent is egregious. Centripetal is informed and believes that Defendants have been aware of Centripetal's products which are marked with its patents. For example, Centripetal builds and sells RuleGATE 2000, a product which is marked with at least the '722 Patent, '370 Patent, '205 Patent, the '213 Patent, and the '077 Patent. Despite their knowledge of Centripetal and its patents, Centripetal is informed and believes that Defendant's deliberately copied Centripetal's patented technology, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000, which Defendants implemented into their products and services. The blatant copying of Centripetal's patented technology is egregious behavior warranting a finding of willful infringement and enhanced damages.

86. This further demonstrates that Defendants knew or, in the alternative, was willfully blind to Centripetal's Asserted Patents. Despite this knowledge and/or willful blindness, Defendants have acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

87. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '722 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '722 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '722 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

FIFTH CAUSE OF ACTION
(Patent Infringement of the '213 Patent)

88. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth

herein, the allegations of the preceding paragraphs, as set forth above.

89. Defendants have infringed and continues to infringe Claims 1-16 of the '213 Patent in violation of 35 U.S.C. § 271(a).

90. Defendants' infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

91. Defendants' acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

92. Defendants' infringement includes the manufacture, use, sale, importation and/or offer for sale of Defendants' products and services, including but not limited to the Ixia ThreatARMOR, Vision ONE devices, Application and Threat Intelligence servers, alone or in conjunction with one another (collectively, the "Accused '213 Products").

93. For example, Defendants have infringed, and continue to infringe, at least claim 1 of the '213 patent:

> 1. 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;
>
> receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;
>
> 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;

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

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;

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

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

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.

94. The Accused '213 Products practice "[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":

95. The Accused '213 Products include the Application and Threat Intelligence Processor ("ATIP"), which receives information from Ixia's Application and Threat Intelligence ("ATI"), which provides "Continuous Real-Time Data Feeds to Ensure Current Application and Threat Intelligence at All Times." *See* https://www.ixiacom.com/products/application-and-threat-intelligence-subscription at 1, attached hereto as Exhibit U. "ATI technology is leveraged

across Ixia's visibility, test, and security portfolio" and include "Real-time cloud threat intelligence that enables Ixia's ThreatARMOR to provide continuous protection, filtering out untrusted countries, malicious sites, and harmful IP addresses (malware distribution, phishing sites, botnet C&C sites, spam distribution, bogons, hijacked domains, and unassigned IPs)," "Application insight enabling ATIP and Ixia's network-visibility products to provide complete network visibility extending beyond Layer 4 into granular application behaviors, including an always-on global IP geolocation database and an evergreen feed for ATIP to provide constant updates for the top applications critical in validating lawful intercept (LI), data loss prevention (DLP), and deep packet inspection (DPI) devices," "Real-World Traffic™ that provides current simulations of 100+ evasion techniques and information to recreate network traffic using more than 300+ applications, updated with the Breaking Point subscription," and "Continually updated ATI application library, is used by Ixia's IxLoad, IxNetwork, and IxChariot test solutions, helps users validate the scale and performance capabilities of content-aware devices and networks." *See* https://www.ixiacom.com/products/application-and-threat-intelligence-subscription at 3, attached hereto as Exhibit U.

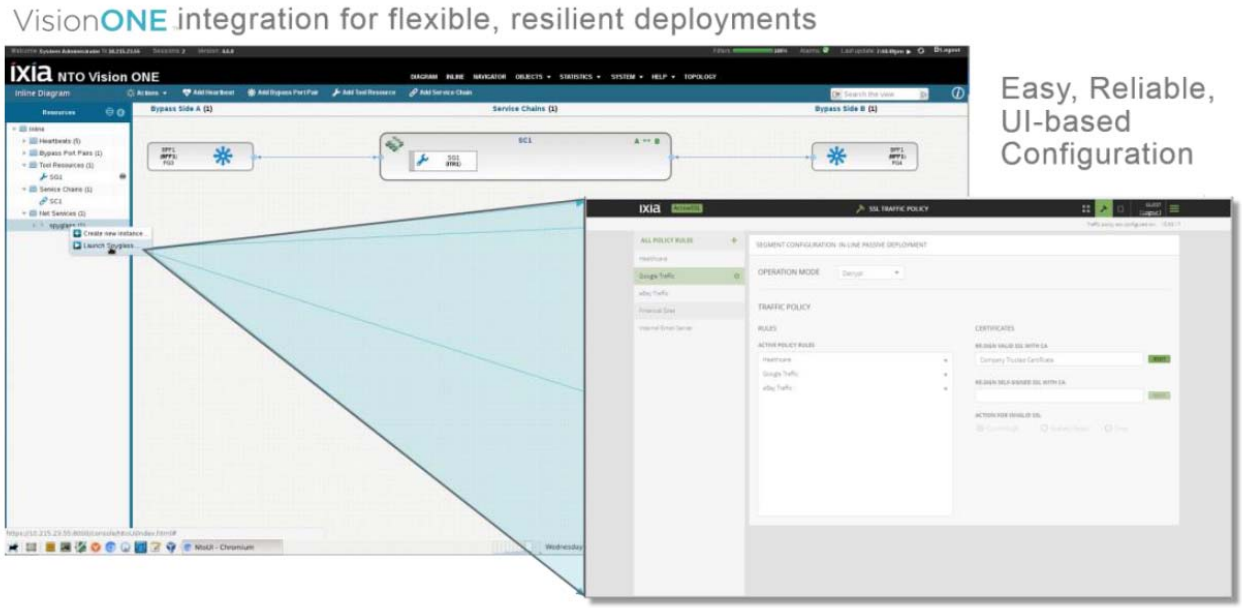
96. The Accused '213 Products include AppStack, comprising the Deep Packet Inspection ("DPI") feature, which "classifies traffic in real time and directs it to the correct tool according to parameters such as application type, geolocation, or even handset type—so tools get just the traffic type they need, again optimizing your investment in tool infrastructure."

APPSTACK (ATIP) CAPABILITIES

- Performs DPI to identify traffic per:
  - Application, geography, device information, and service provider
  - Application signatures are regularly updated via ATI subscription
- Regular expression matching
- Multiple actions can be taken on matching sessions
  - Forward all related packets to an analysis tool
  - Enhanced NetFlow v9 and v10 and IPFIX can be generated and sent to up to 10 collectors

Ixia-V-DS-Vision-ONE_0.pdf at 2, attached hereto as Exhibit V.

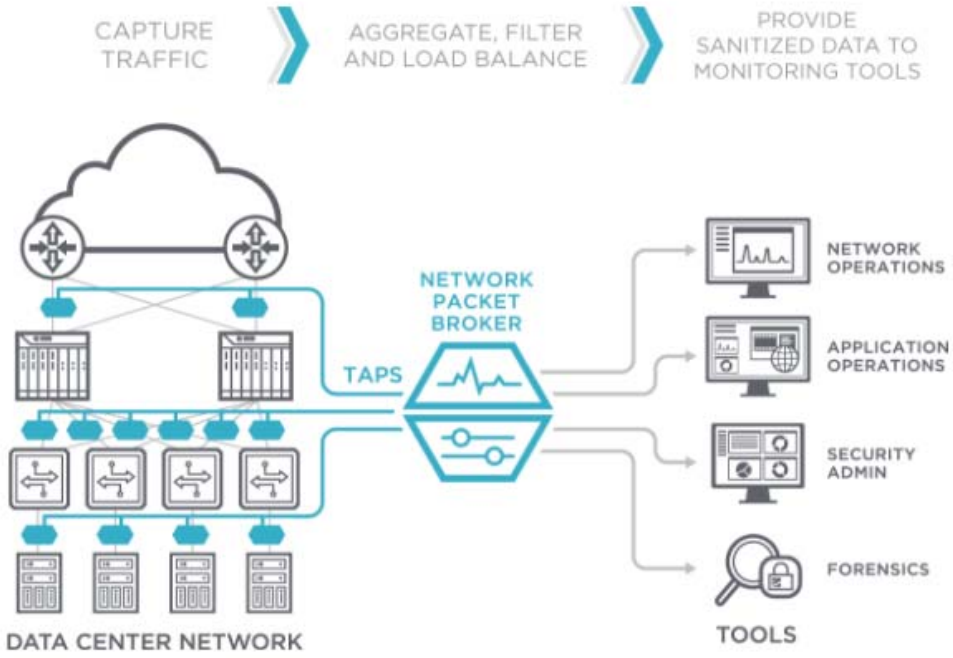
97. The Accused '213 Products include an "Easy, Reliable, UI-based configuration" tool which includes "Traffic Policy" rules for packets and "[e]vent monitoring and logging" capabilities. Ixia-V-DS-Vision-ONE_0.pdf at 4-5, attached hereto as Exhibit V.



Ixia-V-DS-Vision-ONE_0.pdf at 4, attached hereto as Exhibit V.

98. The Accused '213 Products practice "receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway." The Accused '213 Products "provide real-time, end-to-end visibility,

insight and security into physical, virtual, SDN and NFV networks, delivering the control, coverage and performance in a seamless fashion to protect and improve crucial networking, data center and cloud business assets." The Accused '213 Products may "[c]apture all your network traffic by tapping every network link," and "traffic flows to one or more Vision network packet brokers." *See* https://www.ixiacom.com/products-services/visibility at 1, attached hereto as Exhibit W.



See https://www.ixiacom.com/products-services/visibility at 1, attached hereto as Exhibit W.

99. The Accused '213 Products practice "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."

100. The Accused '213 Products include AppStack, comprising the Deep Packet Inspection ("DPI") feature, which "classifies traffic in real time and directs it to the correct tool

according to parameters such as application type, geolocation, or even handset type—so tools get just the traffic type they need, again optimizing your investment in tool infrastructure."

APPSTACK (ATIP) CAPABILITIES

- Performs DPI to identify traffic per:
  - Application, geography, device information, and service provider
  - Application signatures are regularly updated via ATI subscription
- Regular expression matching
- Multiple actions can be taken on matching sessions
  - Forward all related packets to an analysis tool
  - Enhanced NetFlow v9 and v10 and IPFIX can be generated and sent to up to 10 collectors

Ixia-V-DS-Vision-ONE_0.pdf at 2, attached hereto as Exhibit V.

101. The Accused '213 Products practice "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: 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; 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 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."

102. The Accused '213 Products include AppStack, comprising the Deep Packet Inspection ("DPI") feature, which "classifies traffic in real time and directs it to the correct tool according to parameters such as application type, geolocation, or even handset type—so tools get just the traffic type they need, again optimizing your investment in tool infrastructure."

APPSTACK (ATIP) CAPABILITIES

- Performs DPI to identify traffic per:
  - Application, geography, device information, and service provider
  - Application signatures are regularly updated via ATI subscription
- Regular expression matching
- Multiple actions can be taken on matching sessions
  - Forward all related packets to an analysis tool
  - Enhanced NetFlow v9 and v10 and IPFIX can be generated and sent to up to 10 collectors

Ixia-V-DS-Vision-ONE_0.pdf at 2, attached hereto as Exhibit V.

103. The Accused '213 Products include PacketStack, which includes packet filtering features such as Header Stripping, Packet Trimming, Timestamping, Data Masking, and GRE Tunneling. Header Stripping "[d]etect[s] and remove[s] [packet] headers so data can be easily analyzed by security and monitoring (IPS, IDS, NGFW, etc.) tools that do not support such protocols." *See* https://www.ixiacom.com/products/packetstack, attached hereto as Exhibit X.

HEADER (PROTOCOL) STRIPPING

Detect and remove headers so data can be easily analyzed by security and monitoring (IPS, IDS, NGFW, etc.) tools that do not support such protocols

- Protocols and headers removed: Cisco Fabric path, VLAN or QinQ, VNTag, GTP, VXLAN, L2GRE/NVGRE, MPLS – L2VPN/VPLS with or without Control Word, L3VPN

See https://www.ixiacom.com/products/packetstack, attached hereto as Exhibit X.

104. The Accused '213 Products perform Packet Trimming, which "cut[s] out the unnecessary information and reduc[es] packet size" from packets. *See* https://www.ixiacom.com/products/packetstack, attached hereto as Exhibit X.

PACKET TRIMMING

Send only what security and monitoring tools need by cutting out the unnecessary information and reducing packet size

- Improve security by protecting sensitive user data – remove personally identifiable information (PII) for PCI compliance
- Increase tool efficiency, by reducing average frame length by 75%
- Trim packets from 64-16342 bytes and using many offset templates (MAC, VLAN, MPLS, etc)
- Original packet length can be retained as part of Ixia trailer

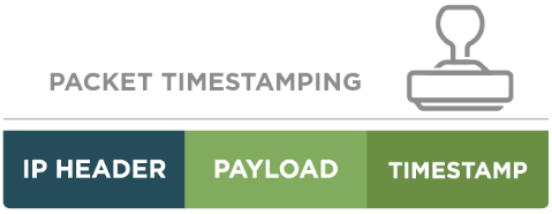
See https://www.ixiacom.com/products/packetstack, attached hereto as Exhibit X.

105. The Accused '213 Products perform Timestamping, which "insert[s] a high-accuracy timestamp into every packet at ingress."

TIMESTAMPING

Network operators require high-accuracy timestamps on packets to correlate events with other device logs in low-latency financial data centers and to correlate traffic events across a WAN. With this feature, you can insert a high-accuracy timestamp into every packet at ingress.

- Timestamp sources include local, PTP and NTP
- Highly accurate – nanoseconds
- Support timestamping at all speeds (1/10/40/100G)
- Support for Wireshark, Riverbed, Corvil, and other popular analysis tools



See https://www.ixiacom.com/products/packetstack, attached hereto as Exhibit X.

106. The Accused '213 Products perform Data Masking, which "hide[s] or overwrite[s] sensitive or personally identifiable information (PII) before providing the data to analysis tools."

DATA MASKING

Hide or overwrite sensitive or personally identifiable information (PII) before providing the data to analysis tools. Achieve regulatory compliance for HIPAA, PCI-DSS financial transactions and more

- Hide information you want to protect
- Keep your customers and other info secure
- Overwrite packet with **any number** of bytes at user configurable offset
- Predefined offset templates for easy header skipping (start of L2, end of L2, end of L3)
- For pre-defined credit card and other templates, check out Data Masking Plus, a part of AppStack

See https://www.ixiacom.com/products/packetstack, attached hereto as Exhibit X.

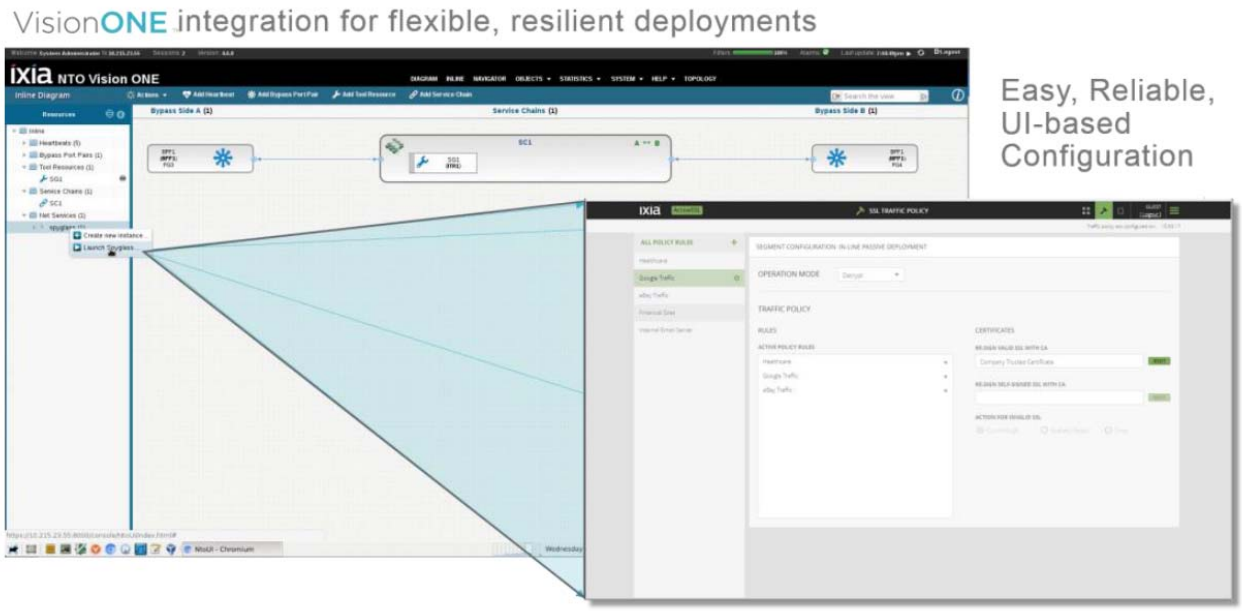
107. The Accused '213 Products "provides easy-to-use graphical displays of the traffic captured."

Ixia's Application and Threat Intelligence Processor (ATIP) provides easy-to-use graphical displays of the traffic captured by Vision ONE

Ixia-V-DS-Vision-ONE_0.pdf at 3, attached hereto as Exhibit V.

108. The Accused '213 Products include an "Easy, Reliable, UI-based configuration"

tool which includes "Traffic Policy" rules for packets and "[e]vent monitoring and logging" capabilities. Ixia-V-DS-Vision-ONE_0.pdf at 4-5, attached hereto as Exhibit V.



Ixia-V-DS-Vision-ONE_0.pdf at 4, attached hereto as Exhibit V.

109. The Accused '213 Products practice "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."

110. The Accused '213 Products include AppStack, comprising the Deep Packet Inspection ("DPI") feature, which "classifies traffic in real time and directs it to the correct tool according to parameters such as application type, geolocation, or even handset type—so tools get just the traffic type they need, again optimizing your investment in tool infrastructure."

APPSTACK (ATIP) CAPABILITIES

- Performs DPI to identify traffic per:
  - Application, geography, device information, and service provider
  - Application signatures are regularly updated via ATI subscription
- Regular expression matching
- Multiple actions can be taken on matching sessions
  - Forward all related packets to an analysis tool
  - Enhanced NetFlow v9 and v10 and IPFIX can be generated and sent to up to 10 collectors

Ixia-V-DS-Vision-ONE_0.pdf at 2, attached hereto as Exhibit V.

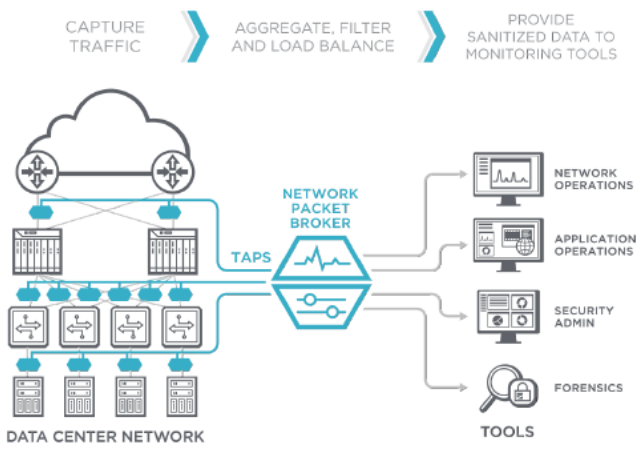
111. The Accused '213 Products "provide sanitized data to monitoring tools." As shown below, "[y]our security, performance and monitoring tools receive the most appropriate data stream, tailored specifically for that tool; your tools work more efficiently, and most effectively."

Ixia Visibility Solutions provide real-time, end-to-end visibility, insight and security into physical, virtual, SDN and NFV networks, delivering the control, coverage and performance in a seamless fashion to protect and improve crucial networking, data center and cloud business assets.

Step 1: Capture all your network traffic by tapping every network link

Step 2: Through non-production links, traffic flows to one or more Vision network packet brokers where duplicate data is removed then filtered using NetStack, PacketStack, SecureStack and AppStack visibility intelligence capabilities

Step 3: Your security, performance and monitoring tools receive the most appropriate data stream, tailored specifically for that tool; your tools work more efficiently, and most effectively



See https://www.ixiacom.com/products-services/visibility at 1, attached hereto as Exhibit W.

112. As a result of Defendants' unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

113. Defendants' infringement of the '213 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

114. Defendants have willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Defendants had knowledge of the Asserted Patents through various channels and despite their knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

115. On or around July 2014, employees from Anue Systems, Inc., a company Ixia acquired in 2012, visited Centripetal's website at least as early as 2014 and have continued to the present. *See, e.g.*, LeadLander Daily Report - Anue Systems 07-31-2014.pdf, attached hereto as Exhibit K; LeadLander Alert - Anue Systems 11-20-2014.pdf, attached hereto as Exhibit L; LeadLander Alert - Anue Systems 11-17-2015.pdf, attached hereto as Exhibit M. Website tracking reports indicate that those employees regularly viewed Centripetal's web pages, including the specific pages explaining that Centripetal's technology was protected by numerous patents. For example, reports indicate that Scott Register, who was previously Sr. Director of Product Management for Ixia's Anue Net Tool Optimizer and is now Ixia's current Vice President of Product Management "leading the development of new Ixia products in the areas of Security, Virtualization and Cloud" regularly viewed Centripetal's web pages. *See, e.g.*, https://www.ixiacom.com/person/scott-register, attached hereto as Exhibit N; Ixia Leadlander (Scot Register).pdf, attached hereto as Exhibit O. Mr. Register has regularly promoted the Accused Products, including the ThreatARMOR devices. *Id.*

116. Further, on May 2, 2016, in an article written by Jon Oltsik in *Network World* titled "The Rise of Threat Intelligence Gateways," Mr. Oltsik detailed functions of threat intelligence gateways provided by a number of vendors, including Centripetal. *See* J. Ostik,

"The rise of threat intelligence gateways," available at https://www.csoonline.com/article/3064299/security/the-rise-of-threat-intelligence-gateways.html, attached hereto as Exhibit P. Defendants use several quotes from Mr. Oltsik on their web sites, including, for example, at https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T. Moreover, Defendants have held webinars with Mr. Oltsik to promote their products.

117. Defendants thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents.

118. Defendants' infringement of the '213 Patent is egregious. Centripetal is informed and believes that Defendants have been aware of Centripetal's products which are marked with its patents. For example, Centripetal builds and sells RuleGATE 2000, a product which is marked with at least the '722 Patent, '370 Patent, '205 Patent, the '213 Patent, and the '077 Patent. Despite their knowledge of Centripetal and its patents, Centripetal is informed and believes that Defendant's deliberately copied Centripetal's patented technology, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000, which Defendants implemented into their products and services. The blatant copying of Centripetal's patented technology is egregious behavior warranting a finding of willful infringement and enhanced damages.

119. This further demonstrates that Defendants knew or, in the alternative, was willfully blind to Centripetal's Asserted Patents. Despite this knowledge and/or willful blindness, Defendants have acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

120. Centripetal is informed and believes that Defendants have undertaken no efforts

to design these products or services around the '213 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '213 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '213 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

SIXTH CAUSE OF ACTION
(Indirect Infringement of the '213 Patent pursuant to 35 U.S.C. § 271(b))

121. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

122. Defendants have induced and continues to induce infringement of one or more claims of the '213 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the '213 Patent, Defendants indirectly infringes the '213 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '213 Patent, where all the steps of the method claims are performed by either Defendants, its customers, purchasers, users or developers, or some combination thereof. Defendants knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '213 Patent, including Claims 1-16.

123. Defendants knowingly and actively aided and abetted the direct infringement of the '213 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '213 Accused Products. Such instructions and encouragement include, but are not

limited to, advising third parties to use the '213 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '213 Patent, specifically through the use of the Ixia ThreatARMOR, Vision ONE devices, Application and Threat Intelligence servers, alone or in conjunction with one another, and by advertising and promoting the use of the '213 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '213 Accused Products in an infringing manner.

124. Defendants update and maintain an HTTP site with Defendants' quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets, test plans, and application notes which cover in depth aspects of operating Defendants' offerings. *See* https://support.ixiacom.com/, attached hereto as Exhibit Y.

125. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '213 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '213 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '213 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

SEVENTH CAUSE OF ACTION
(Patent Infringement of the '856 Patent)

126. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

127. Defendants have infringed and continues to infringe Claims 1-25 of the '856 Patent in violation of 35 U.S.C. § 271(a).

128. Defendants' infringement is based upon literal infringement or infringement

under the doctrine of equivalents, or both.

129. Defendants' acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

130. Defendants' infringement includes the manufacture, use, sale, importation and/or offer for sale of Defendants' products and services, including but not limited to the Ixia ThreatARMOR, Vision ONE devices, Application and Threat Intelligence servers, alone or in conjunction with one another (collectively, the "Accused '856 Products").

131. For example, Defendants have infringed, and continue to infringe, at least claim 1 of the '856 patent:

> 1. A method, comprising:
>
> receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;
>
> identifying packets comprising unencrypted data;
>
> identifying packets comprising encrypted data;
>
> determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;
>
> filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:
>
> packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-

threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

132. The Accused '856 Products practice "receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat."

133. The Accused '856 Products include the Application and Threat Intelligence Processor ("ATIP"), which receives information from Ixia's Application and Threat Intelligence ("ATI"), which provides "Continuous Real-Time Data Feeds to Ensure Current Application and Threat Intelligence at All Times." *See* https://www.ixiacom.com/products/application-and-threat-intelligence-subscription at 1, attached hereto as Exhibit U. "ATI technology is leveraged across Ixia's visibility, test, and security portfolio" and include "Real-time cloud threat intelligence that enables Ixia's ThreatARMOR to provide continuous protection, filtering out untrusted countries, malicious sites, and harmful IP addresses (malware distribution, phishing sites, botnet C&C sites, spam distribution, bogons, hijacked domains, and unassigned IPs)," "Application insight enabling ATIP and Ixia's network-visibility products to provide complete network visibility extending beyond Layer 4 into granular application behaviors, including an always-on global IP geolocation database and an evergreen feed for ATIP to provide constant updates for the top applications critical in validating lawful intercept (LI), data loss prevention

(DLP), and deep packet inspection (DPI) devices," "Real-World Traffic™ that provides current simulations of 100+ evasion techniques and information to recreate network traffic using more than 300+ applications, updated with the Breaking Point subscription," and "Continually updated ATI application library, is used by Ixia's IxLoad, IxNetwork, and IxChariot test solutions, helps users validate the scale and performance capabilities of content-aware devices and networks." *See* https://www.ixiacom.com/products/application-and-threat-intelligence-subscription at 3, attached hereto as Exhibit U.

134. The Accused '856 Products practice "identifying packets comprising unencrypted data" and "identifying packets comprising encrypted data." The Accused '856 Products include Active SSL, which "enables organizations to see inside traffic that uses ephemeral key cryptography."

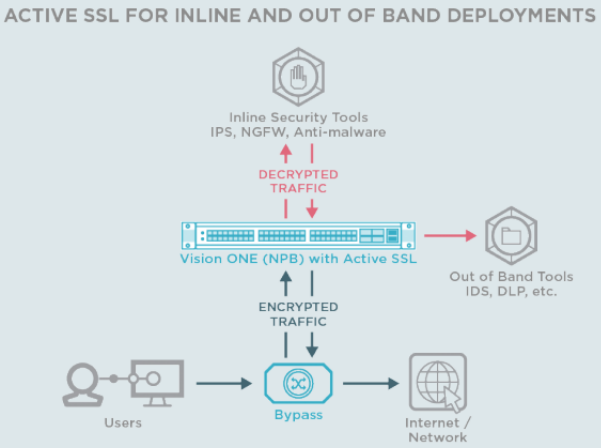
ACTIVE SSL

Now Available for Vision ONE!

Ixia's Active SSL capability, an addition to its SecureStack feature set, enables organizations to see inside traffic that uses ephemeral key cryptography.

Ixia's Active SSL can be used both inline and out-of-band, for outbound and inbound traffic and simultaneously with NetStack, PacketStack and AppStack capabilities. The Active SSL capability will be available via a high-performance application module that is compatible with Vision ONE™. **With a dedicated cryptographic processor, it provides the best throughput integrated with a visibility solution**. Moreover, it includes built-in policy management, URL categorization, **support for all leading ciphers** and reporting.

Learn more about Ixia's Active SSL



https://www.ixiacom.com/products/vision-one at 1-2, attached hereto as Exhibit Q.

135. The Accused '856 Products practice "determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that

corresponds to the one or more network-threat indicators."

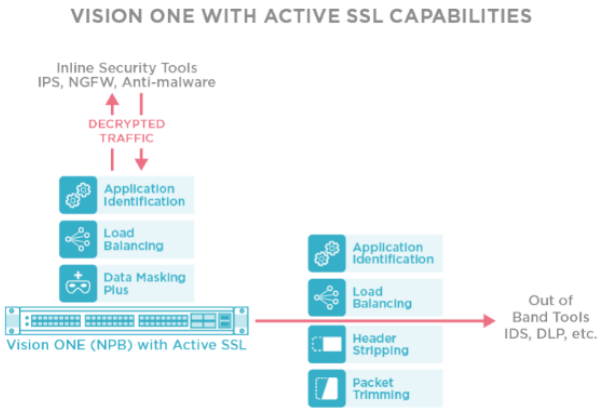
136. The Accused '856 Products include "Active SSL with Ixia's NetStack, PacketStack, and AppStack capabilities for flexibility and limitless visibility. With Ixia, traffic can be decrypted and then packets trimmed, headers stripped and more, before sending to out-of-band security tools. This increases tool efficiency and operating life. For inline deployments, decryption and filtering can happen in any order. Using Application Identification, packets can be selectively filtered based on application, browser, OS or more and then decrypted for inspection. Using application identification helps minimize impact by only decrypting relevant traffic, so security and monitoring tools only get relevant traffic. Traffic can also be decrypted and then personally identifiable information (PII) can be masked with Data Masking Plus to protect users and organizations." *See* https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 3, attached hereto as Exhibit Z.

Use Active SSL with Ixia's NetStack, PacketStack and AppStack capabilities for flexibility and limitless visibility.

With Ixia, traffic can be decrypted and then packets trimmed, headers stripped and more, before sending to out-of-band security tools. This increases tool efficiency and operating life.

For inline deployments, decryption and filtering can happen in any order. Using Application Identification, packets can be selectively filtered based on application, browser, OS or more and then decrypted for inspection. Using application identification helps minimize impact by only decrypting relevant traffic, so security and monitoring tools only get relevant traffic. Traffic can also be decrypted and then personally identifiable information (PII) can be masked with Data Masking Plus to protect users and organizations.

Using many features concurrently ensures optimized security policy enforcement, while allowing tools to operate efficiently. Improving the life of security and monitoring tools.



See https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 3, attached hereto as Exhibit Z.

137. The Accused '856 Products include AppStack, comprising the Deep Packet Inspection ("DPI") feature, which "classifies traffic in real time and directs it to the correct tool

according to parameters such as application type, geolocation, or even handset type—so tools get just the traffic type they need, again optimizing your investment in tool infrastructure."

APPSTACK (ATIP) CAPABILITIES

- Performs DPI to identify traffic per:
  - Application, geography, device information, and service provider
  - Application signatures are regularly updated via ATI subscription
- Regular expression matching
- Multiple actions can be taken on matching sessions
  - Forward all related packets to an analysis tool
  - Enhanced NetFlow v9 and v10 and IPFIX can be generated and sent to up to 10 collectors

Ixia-V-DS-Vision-ONE_0.pdf at 2, attached hereto as Exhibit V.

138. The Accused '856 Products practice "filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators."

139. The Accused '856 Products include Active SSL, which "supports all leading ciphers that are indicated in the TLS 1.3 draft. As the draft evolves and is released, Ixia will continue to add support for leading ciphers." Ixia-V-DS-Vision-ONE_0.pdf at 4, attached hereto as Exhibit V.

SUPPORTS LEADING CIPHERS

Active SSL supports all leading ciphers that are indicated in the TLS 1.3 draft. As the draft evolves and is released, Ixia will continue to add support for leading ciphers.

Supported Ciphers		Kx	Au	Enc	Mac
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH	RSA	AESGCM(128)	AEAD
ECDHE-ECDSA-AES128-SHA	SSLv3	ECDH	ECDSA	AES(128)	SHA1
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	ECDH	ECDSA	AESGCM(128)	AEAD
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	DH	RSA	AESGCM(128)	AEAD
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	DH	RSA	AESGCM(256)	AEAD
ECDHE-RSA-AES128-SHA256	TLSv1.2	ECDH	RSA	AES(128)	SHA256
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	ECDH	ECDSA	AES(128)	SHA256
ECDHE-RSA-AES128-SHA	SSLv3	ECDH	RSA	AES(128)	SHA1
DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES(256)	SHA1
ECDHE-RSA-DES-CBC3-SHA	SSLv3	ECDH	RSA	3DES(168)	SHA1
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	ECDH	ECDSA	3DES(168)	SHA1
AES128-GCM-SHA256	TLSv1.2	RSA	RSA	AESGCM(128)	AEAD
AES256-GCM-SHA384	TLSv1.2	RSA	RSA	AESGCM(256)	AEAD
AES128-SHA256	TLSv1.2	RSA	RSA	AES(128)	SHA256
AES256-SHA256	TLSv1.2	RSA	RSA	AES(256)	SHA256
AES128-SHA	SSLv3	RSA	RSA	AES(128)	SHA1
AES256-SHA	SSLv3	RSA	RSA	AES(256)	SHA1
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES(256)	SHA1
DHE-RSA-AES128-SHA256	TLSv1.2	DH	RSA	AES(128)	SHA256
DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES(128)	SHA1
DHE-RSA-AES256-SHA256	TLSv1.2	DH	RSA	AES(256)	SHA256

Ixia-V-DS-Vision-ONE_0.pdf at 4, attached hereto as Exhibit V.

140. The Accused '856 Products include Active SSL, which "includes built-in policy management, Uniform Resource Locator (URL) categorization, support for all leading ciphers and reporting." *See* https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 1, attached hereto as Exhibit Z.

IXIA'S ACTIVE SSL

As most traffic becomes encrypted and with ephemeral key on its way to becoming the dominant technology, organizations need a way to retain the benefits of Transport Layer Security (TLS) 1.3, while being able to inspect traffic for threats and malware to protect their networks and users.

Ixia's Active Secure Sockets Layer (SSL) capability, an addition to its SecureStack feature set, enables organizations to see inside traffic that uses ephemeral key cryptography through its visibility platform. Ixia's Active SSL can be used both inline and out-of-band, for outbound and inbound traffic and it can be used simultaneously with NetStack, PacketStack and AppStack capabilities. The Active SSL capability will be available via a high-performance application module that is compatible with Vision ONE™, a turnkey network packet broker that provides high-performance, lossless visibility. **With a dedicated cryptographic processor, Active SSL provides the best throughput integrated with a visibility solution**. Moreover, it includes built-in policy management, Uniform Resource Locator (URL) categorization, **support for all leading ciphers** and reporting.

See https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 1, attached hereto as Exhibit Z.

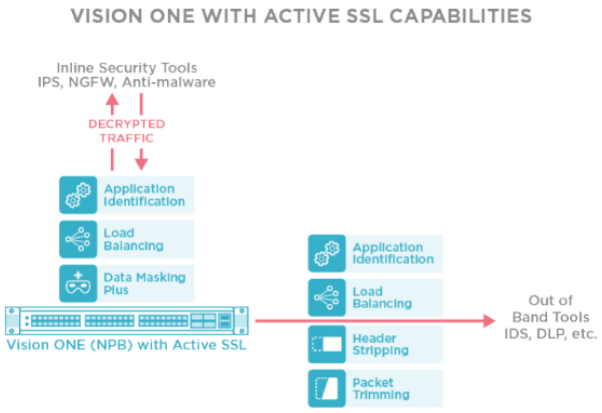
141. The Accused '856 Products include "Active SSL with Ixia's NetStack, PacketStack, and AppStack capabilities for flexibility and limitless visibility. With Ixia, traffic can be decrypted and then packets trimmed, headers stripped and more, before sending to out-of-band security tools. This increases tool efficiency and operating life. For inline deployments, decryption and filtering can happen in any order. Using Application Identification, packets can be selectively filtered based on application, browser, OS or more and then decrypted for inspection. Using application identification helps minimize impact by only decrypting relevant traffic, so security and monitoring tools only get relevant traffic. Traffic can also be decrypted and then personally identifiable information (PII) can be masked with Data Masking Plus to protect users and organizations." *See* https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 3, attached hereto as Exhibit Z.

Use Active SSL with Ixia's NetStack, PacketStack and AppStack capabilities for flexibility and limitless visibility.

With Ixia, traffic can be decrypted and then packets trimmed, headers stripped and more, before sending to out-of-band security tools. This increases tool efficiency and operating life.

For inline deployments, decryption and filtering can happen in any order. Using Application Identification, packets can be selectively filtered based on application, browser, OS or more and then decrypted for inspection. Using application identification helps minimize impact by only decrypting relevant traffic, so security and monitoring tools only get relevant traffic. Traffic can also be decrypted and then personally identifiable information (PII) can be masked with Data Masking Plus to protect users and organizations.

Using many features concurrently ensures optimized security policy enforcement, while allowing tools to operate efficiently. Improving the life of security and monitoring tools.



See https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 3, attached hereto as Exhibit Z.

142. The Accused '856 Products include AppStack, comprising the Deep Packet Inspection ("DPI") feature, which "classifies traffic in real time and directs it to the correct tool

according to parameters such as application type, geolocation, or even handset type—so tools get just the traffic type they need, again optimizing your investment in tool infrastructure."

APPSTACK (ATIP) CAPABILITIES

• Performs DPI to identify traffic per:
  ○ Application, geography, device information, and service provider
  ○ Application signatures are regularly updated via ATI subscription
• Regular expression matching
• Multiple actions can be taken on matching sessions
  ○ Forward all related packets to an analysis tool
  ○ Enhanced NetFlow v9 and v10 and IPFIX can be generated and sent to up to 10 collectors

Ixia-V-DS-Vision-ONE_0.pdf at 2, attached hereto as Exhibit V.

143. The Accused '856 Products practice "routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators."

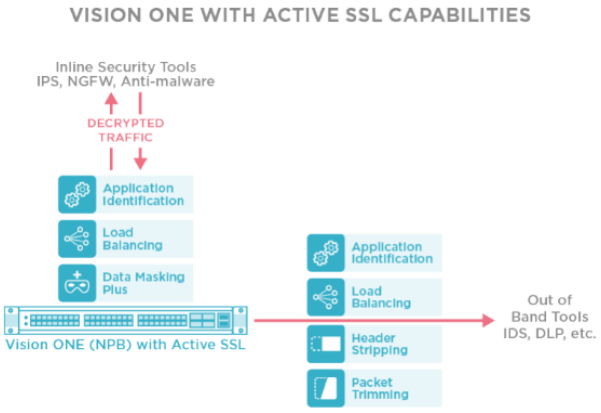
144. The Accused '856 Products include "Active SSL with Ixia's NetStack, PacketStack, and AppStack capabilities for flexibility and limitless visibility. With Ixia, traffic can be decrypted and then packets trimmed, headers stripped and more, before sending to out-of-band security tools. This increases tool efficiency and operating life. For inline deployments, decryption and filtering can happen in any order. Using Application Identification, packets can be selectively filtered based on application, browser, OS or more and then decrypted for inspection. Using application identification helps minimize impact by only decrypting relevant traffic, so security and monitoring tools only get relevant traffic. Traffic can also be decrypted and then personally identifiable information (PII) can be masked with Data Masking Plus to protect users and organizations." *See* https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 3, attached hereto as Exhibit Z.

Use Active SSL with Ixia's NetStack, PacketStack and AppStack capabilities for flexibility and limitless visibility.

With Ixia, traffic can be decrypted and then packets trimmed, headers stripped and more, before sending to out-of-band security tools. This increases tool efficiency and operating life.

For inline deployments, decryption and filtering can happen in any order. Using Application Identification, packets can be selectively filtered based on application, browser, OS or more and then decrypted for inspection. Using application identification helps minimize impact by only decrypting relevant traffic, so security and monitoring tools only get relevant traffic. Traffic can also be decrypted and then personally identifiable information (PII) can be masked with Data Masking Plus to protect users and organizations.

Using many features concurrently ensures optimized security policy enforcement, while allowing tools to operate efficiently. Improving the life of security and monitoring tools.



See https://www.ixiacom.com/tls-and-ssl-decryption-and-encryption at 3, attached hereto as Exhibit Z.

145. The Accused '856 Products include AppStack, comprising the Deep Packet Inspection ("DPI") feature, which "classifies traffic in real time and directs it to the correct tool according to parameters such as application type, geolocation, or even handset type—so tools get just the traffic type they need, again optimizing your investment in tool infrastructure."

APPSTACK (ATIP) CAPABILITIES

- Performs DPI to identify traffic per:
  - Application, geography, device information, and service provider
  - Application signatures are regularly updated via ATI subscription
- Regular expression matching
- Multiple actions can be taken on matching sessions
  - Forward all related packets to an analysis tool
  - Enhanced NetFlow v9 and v10 and IPFIX can be generated and sent to up to 10 collectors

Ixia-V-DS-Vision-ONE_0.pdf at 2, attached hereto as Exhibit V.

146. Defendants' infringement of the '856 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

147. Defendants have willfully infringed each of the Asserted Patents. Centripetal is

informed and believes that Defendants had knowledge of the Asserted Patents through various channels and despite their knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

148. On or around July 2014, employees from Anue Systems, Inc., a company Ixia acquired in 2012, visited Centripetal's website at least as early as 2014 and have continued to the present. *See, e.g.*, LeadLander Daily Report - Anue Systems 07-31-2014.pdf, attached hereto as Exhibit K; LeadLander Alert - Anue Systems 11-20-2014.pdf, attached hereto as Exhibit L; LeadLander Alert - Anue Systems 11-17-2015.pdf, attached hereto as Exhibit M. Website tracking reports indicate that those employees regularly viewed Centripetal's web pages, including the specific pages explaining that Centripetal's technology was protected by numerous patents. For example, reports indicate that Scott Register, who was previously Sr. Director of Product Management for Ixia's Anue Net Tool Optimizer and is now Ixia's current Vice President of Product Management "leading the development of new Ixia products in the areas of Security, Virtualization and Cloud" regularly viewed Centripetal's web pages. *See, e.g.*, https://www.ixiacom.com/person/scott-register, attached hereto as Exhibit N; Ixia Leadlander (Scot Register).pdf, attached hereto as Exhibit O. Mr. Register has regularly promoted the Accused Products, including the ThreatARMOR devices. *Id.*

149. Further, on May 2, 2016, in an article written by Jon Oltsik in *Network World* titled "The Rise of Threat Intelligence Gateways," Mr. Oltsik detailed functions of threat intelligence gateways provided by a number of vendors, including Centripetal. *See* J. Ostik, "The rise of threat intelligence gateways," available at https://www.csoonline.com/article/3064299/security/the-rise-of-threat-intelligence-gateways.html, attached hereto as Exhibit P. Defendants use several quotes from Mr. Oltsik on

their web sites, including, for example, at https://www.ixiacom.com/products/threatarmor, attached hereto as Exhibit T. Moreover, Defendants have held webinars with Mr. Oltsik to promote their products.

150. Defendants thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents.

151. Defendants' infringement of the '856 Patent is egregious. Centripetal is informed and believes that Defendants have been aware of Centripetal's products which are marked with its patents. For example, Centripetal builds and sells RuleGATE 2000, a product which is marked with at least the '722 Patent, '370 Patent, '205 Patent, the '213 Patent, and the '077 Patent. Despite their knowledge of Centripetal and its patents, Centripetal is informed and believes that Defendant's deliberately copied Centripetal's patented technology, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000, which Defendants implemented into their products and services. The blatant copying of Centripetal's patented technology is egregious behavior warranting a finding of willful infringement and enhanced damages.

152. This further demonstrates that Defendants knew or, in the alternative, was willfully blind to Centripetal's Asserted Patents. Despite this knowledge and/or willful blindness, Defendants have acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

153. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '856 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '856 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately,

and egregiously engage in acts of infringement of the '856 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

EIGHTH CAUSE OF ACTION
(Indirect Infringement of the '856 Patent pursuant to 35 U.S.C. § 271(b))

154. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

155. Defendants have induced and continues to induce infringement of one or more claims of the '856 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the '856 Patent, Defendants indirectly infringes the '856 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '856 Patent, where all the steps of the method claims are performed by either Defendants, its customers, purchasers, users or developers, or some combination thereof. Defendants knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '856 Patent, including Claims 1-23.

156. Defendants knowingly and actively aided and abetted the direct infringement of the '856 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '856 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '856 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '856 Patent, specifically through the use of the Ixia ThreatARMOR, Vision ONE devices, Application and Threat

Intelligence servers, alone or in conjunction with one another, and by advertising and promoting the use of the '856 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '856 Accused Products in an infringing manner.

157. Defendants update and maintain an HTTP site with Defendants' quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets, test plans, and application notes which cover in depth aspects of operating Defendants' offerings. *See* https://support.ixiacom.com/, attached hereto as Exhibit Y.

158. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '856 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '856 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '856 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

NINTH CAUSE OF ACTION
(Indirect Infringement of the '370 Patent pursuant to 35 U.S.C. § 271(b))

159. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

160. Defendants have induced and continues to induce infringement of one or more claims of the '370 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the '370 Patent, Defendants indirectly infringes the '370 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '370 Patent, where all the steps of the method claims are

performed by either Defendants, its customers, purchasers, users or developers, or some combination thereof. Defendants knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '370 Patent, including Claims 1-21, 64-75, 100-110, 133-141, 160-168, and 187-193.

161. Defendants knowingly and actively aided and abetted the direct infringement of the '370 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '370 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '370 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '370 Patent, specifically through the use of the Ixia ThreatARMOR, Vision ONE devices, Application and Threat Intelligence servers, alone or in conjunction with one another, and by advertising and promoting the use of the '370 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '370 Accused Products in an infringing manner.

162. Defendants update and maintain an HTTP site with Defendants' quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets, test plans, and application notes which cover in depth aspects of operating Defendants' offerings. *See* https://support.ixiacom.com/, attached hereto as Exhibit Y.

163. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '370 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '370 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '370 Patent, justifying an award to

Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

TENTH CAUSE OF ACTION
(Indirect Infringement of the '205 Patent pursuant to 35 U.S.C. § 271(b))

164. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

165. Defendants have induced and continues to induce infringement of one or more claims of the '205 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the '205 Patent, Defendants indirectly infringes the '205 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '205 Patent, where all the steps of the method claims are performed by either Defendants, its customers, purchasers, users or developers, or some combination thereof. Defendants knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '205 Patent, including Claims 1-16, 49-62, and 91-92.

166. Defendants knowingly and actively aided and abetted the direct infringement of the '205 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '205 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '205 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '205 Patent, specifically through the use of the Ixia ThreatARMOR, Vision ONE devices, Application and Threat Intelligence servers, alone or in conjunction with one another, and by advertising and promoting

the use of the '205 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '205 Accused Products in an infringing manner.

167. Defendants update and maintain an HTTP site with Defendants' quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets, test plans, and application notes which cover in depth aspects of operating Defendants' offerings. *See* https://support.ixiacom.com/, attached hereto as Exhibit Y.

168. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '205 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '205 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '205 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

ELEVENTH CAUSE OF ACTION
(Indirect Infringement of the '077 Patent pursuant to 35 U.S.C. § 271(b))

169. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

170. Defendants have induced and continues to induce infringement of one or more claims of the '077 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the '077 Patent, Defendants indirectly infringes the '077 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '077 Patent, where all the steps of the method claims are performed by either Defendants, its customers, purchasers, users or developers, or some

combination thereof. Defendants knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '077 Patent, including Claims 1-6 and 19-20.

171. Defendants knowingly and actively aided and abetted the direct infringement of the '077 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '077 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '077 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '077 Patent, specifically through the use of the Ixia ThreatARMOR, Vision ONE devices, Application and Threat Intelligence servers, alone or in conjunction with one another, and by advertising and promoting the use of the '077 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '077 Accused Products in an infringing manner.

172. Defendants update and maintain an HTTP site with Defendants' quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets, test plans, and application notes which cover in depth aspects of operating Defendants' offerings. *See* https://support.ixiacom.com/, attached hereto as Exhibit Y.

173. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '077 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '077 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '077 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred

under 35 U.S.C. § 285.

TWELFTH CAUSE OF ACTION
(Indirect Infringement of the '722 Patent pursuant to 35 U.S.C. § 271(b))

174. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

175. Defendants have induced and continues to induce infringement of one or more claims of the '722 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the '722 Patent, Defendants indirectly infringes the '722 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '722 Patent, where all the steps of the method claims are performed by either Defendants, its customers, purchasers, users or developers, or some combination thereof. Defendants knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '722 Patent, including Claims 1-25.

176. Defendants knowingly and actively aided and abetted the direct infringement of the '722 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '722 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '722 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '722 Patent, specifically through the use of the Ixia ThreatARMOR, Vision ONE devices, Application and Threat Intelligence servers, alone or in conjunction with one another, and by advertising and promoting the use of the '722 Accused Products in an infringing manner, and distributing guidelines and

instructions to third parties on how to use the '722 Accused Products in an infringing manner.

177. Defendants update and maintain an HTTP site with Defendants' quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets, test plans, and application notes which cover in depth aspects of operating Defendants' offerings. *See* https://support.ixiacom.com/, attached hereto as Exhibit Y.

178. Centripetal is informed and believes that Defendants have undertaken no efforts to design these products or services around the '722 Patent to avoid infringement despite Defendants' knowledge and understanding that its products and services infringe the '722 Patent. As such, Defendants have acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '722 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Centripetal prays for relief and judgment as follows:

(A) That Defendants have infringed each and every one of the Asserted Patents;

(B) That Defendants, their officers, agents, employees, and those persons in active concert or participation with any of them, and their successors and assigns, be permanently enjoined from infringement of each and every one of the Asserted Patents, including but not limited to an injunction against making, using, selling, and/or offering for sale within the United States, and/or importing into the United States, any products and/or services that infringe the Asserted Patents;

(C) That Centripetal be awarded all damages sufficient to compensate Centripetal for Defendants' infringement of the Asserted Patents, including lost profits suffered by Centripetal

as a result of Defendants' infringement and in an amount not less than a reasonable royalty;

(D) A determination that Defendants' infringement has been willful, wanton, deliberate, and egregious;

(E) For an award of increased damages in an amount not less than three times the damages assessed for Defendants' infringement of the Asserted Patents, in accordance with 35 U.S.C. § 284;

(F) That this case be declared an exceptional case within the meaning of 35 U.S.C. § 285 and that Centripetal be awarded attorneys' fees, costs, and expenses incurred in connection with this action;

(G) An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the Asserted Patents;

(H) That Centripetal be awarded prejudgment and post-judgment interest; and

(I) That Centripetal be awarded such other and further relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

In accordance with Rule 38 of the Federal Rules of Civil Procedure, Plaintiff respectfully demands a jury trial of all issues triable to a jury in this action.

Dated: June 13, 2018

Respectfully submitted,

/s/ Stephen E. Noona

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Paul J. Andre (*pro hac vice*)
Hannah Y. Lee (*pro hac vice*)
James R. Hannah (*pro hac vice*)
Lisa Kobialka (*pro hac vice*)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
hlee@kramerlevin.com
jhannah@kramerlevin.com
lkobialka@kramerlevin.com

Christina L. Martinez (*pro hac vice*)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
Telephone: (212) 715-9000
Facsimile: (212) 715-8000
cmartinez@kramerlevin.com

Attorneys for Plaintiff,
Centripetal Networks, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on June 13, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will automatically send notification of electronic filing to:

William R. Poynter
Virginia State Bar No. 48672
KALEO LEGAL
4456 Corporation Lane, Suite 135
Virginia Beach, VA 23462
Telephone: (757) 238-6383
Facsimile: (757) 304-6175
wpoynter@kaleolegal.com

Christine M. Morgan (*pro hac vice*)
James A. Daire (*pro hac vice*)
John P. Bovich (*pro hac vice*)
Jonah D. Mitchell (*pro hac vice*)
Doyle B. Johnson (*pro hac vice*)
Christopher J. Pulido (*pro hac vice*)
REED SMITH LLP
101 Second Street, Suite 1800
San Francisco, CA 94105
Telephone: (415) 543-8700
Facsimile: (415) 891-8269
cmorgan@reedsmith.com
jdaire@reedsmith.com
jbovich@reedsmith.com
jmitchell@reedsmith.com
dbjohnson@reedsmith.com
cpulido@reedsmith.com

Attorneys for Defendants
Keysight Technologies, Inc. and Ixia

/s/ Stephen E. Noona

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com