FILED
SEP 17 2018
CLERK, U.S. DISTRICT COURT
NORFOLK, VA

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,

Plaintiff,

v. **Civil Action No. 2:17cv383**

KEYSIGHT TECHNOLOGIES, INC. & IXIA,

Defendants.

OPINION & ORDER

On Friday, August 3, 2018 at 11:00 a.m., the Court conducted a Markman hearing for the purpose of construing twenty-seven (27) disputed terms in the Patents at issue.[1] Upon consideration of the Parties' briefs and oral arguments, the Court ruled from the bench as to the terms at issue. This Opinion and Order details the Court's claim construction.

I. FACTUAL BACKGROUND & PROCEDURAL HISTORY

On July 20, 2017, Centripetal Networks, Inc. ("Centripetal" or "Plaintiff") filed its original complaint alleging that Keysight Technologies, Inc. ("Keysight") and Ixia (collectively "Defendants") have infringed several of Plaintiff's patents. Plaintiff alleged infringement of four (4) of its patents: U.S. Patent No. 9,264,370 (the "'370 Patent"), U.S. Patent No. 9,137,205 (the "'205 Patent"), U.S. Patent No. 9,560,077 (the "'077 Patent"), and U.S. Patent No. 9,413,722 (the "'722 patent") (collectively "the Asserted Patents"). Doc. 1 ("Compl.") ¶¶ 6, 9–15. On September 5, 2017, Defendants filed Motions to Dismiss for failure to State a Claim, a Motion to Dismiss for Improper Venue, and a Motion to Transfer Venue under Section 1404(a). Docs. 20,

[1] At the beginning of the hearing, the parties notified the Court that they had agreed that six (6) of the disputed terms no longer needed to be construed. Therefore, this Opinion & Order only addresses the twenty-one (21) remaining terms.

PAN EX1030
Palo Alto Networks v. Centripetal Networks
IPR2022-00182
Page 00001

23, and 24. On November 15, 2017, the Court entered an Order DENYING Defendants' Motion to Dismiss WITHOUT PREJUDICE and an Order DENYING Defendant's Motion to Dismiss for Improper Venue and Motion to Transfer Venue. Docs. 53, 55. On November 15, 2017, the Court also entered an Order for the parties to confer prior to May 10, 2018 to determine whether a Markman hearing is necessary and preliminarily set a Markman hearing for May 24, 2018. Doc. 52. On November 29, 2017, Defendants filed their Answers to Plaintiff's Complaint. Docs. 61, 62. On February 12, 2018, the Court entered a Stipulated Agreed Order Amending the Court's Markman Order. Doc. 74. On April 9, Plaintiff filed a Motion to Compel Discovery. Doc. 98. On April 16, Plaintiff filed a Motion to Amend/Correct its Complaint. Doc. 100. On April 20, 2018, Plaintiff and Defendants each filed their Claim Construction Briefs. Docs 104, 106. On May 2, 2018, Defendants filed a Motion to Limit the Number of Claims Asserted. Doc. 115. On May 3, 2018, Plaintiff and Defendants each filed Rebuttal Claim Construction Briefs. Docs 117, 119. On May 3, 2018, Defendants also filed a Motion to Strike the Declaration of Dr. Nenad Medvidovic, which was offered in support of Plaintiff's Claim Construction Brief. Doc. 120.

On May 7, 2018, the Markman hearing was reset for July 3, 2018. On May 14, 2018, Defendants filed a Cross-Motion to Compel discovery. Doc. 128. On May 25, 2018, Defendants filed a Motion for Summary Judgment of Invalidity. Doc. 145. On June 1, 2018, the Court set a hearing on Plaintiff's Motions to Compel and to Amend/Correct Complaint and Defendants' Cross-Motion to Compel, Motion to Limit the Number of Claims Asserted, Motion for Summary Judgment, and Motion to Strike the Testimony of Dr. Nedad Medvidovic for June 12, 2018. The Court also entered an Order to Expedite Briefing on Defendants' Motion for Summary Judgment

so that Plaintiff's response was due on June 7, 2018, and Defendant's Reply was due on June 11, 2018. Doc. 163.

At the hearing on June 12, 2018, the Court GRANTED Defendants' Motion to Limit the Number of Claims Asserted. Doc. 198. The Court also GRANTED Plaintiff's Motion to Amend/Correct its Complaint. Id. The Court GRANTED Defendant's Motion to Compel Discovery, IN PART, and the Court RESERVED RULING on Plaintiff's Motion to Compel Discovery, and ORDERED the parties to meet and confer regarding the issues raised in their Motions to Compel. Id. The Court also RESERVED RULING on Defendant's Motion for Summary Judgment and Defendants' Motion to Strike the Declaration of Dr. Nenad Medvidovic. Id. In light of the Plaintiff's Amended Complaint, the Court continued the Markman hearing until August 3, 2018.

On June 13, 2018, Plaintiff filed its Amended Complaint, which alleged that Defendant infringed two (2) additional patents: U.S. Patent No. 9,917,856 ("the '856 patent") and U.S. Patent No. 9,565,213 ("the 213 patent"). Doc. 192. The Amended Complaint also added claims alleging that Defendants willfully infringed each of the Asserted Patents. Id.

On June 18, 2018, the Court entered a Stipulated Order requiring the parties to supplement their Markman briefings by July 20, 2018. On June 28, 2018, Defendants filed their Answers to Plaintiff's Amended Complaint. Docs. 206, 207. On July 12, 2018, Plaintiff filed a Motion to Compel. Doc. 213. Defendants filed a brief in opposition to Plaintiff's Motion to Compel on July 13, 2018. Doc. 222. On July 16, Plaintiff filed a Motion for Protective Order. Doc. 224. On July 19, Plaintiff replied in support of its Motion to Compel. Doc. 235. On July 20, 2018, Plaintiff and Defendants filed their Supplemental Claim Construction Briefs and an Amended Joint Claim Construction and Prehearing Statement. Docs. 240, 241, 244. A hearing

on Plaintiffs' Motion to Compel and Motion for Protective Order is set for August 3, 2018 at the Markman hearing.

II. CLAIMS ASSERTED

A. The '205 Patent

The '205 Patent was issued on September 15, 2015 for an invention entitled "Method and Systems for Protecting a Secured Network." See Am. Compl. ¶ 10. The '205 Patent discloses various methods by which a device is programmed to perform protective functions on incoming packets. See Am. Compl., Ex. B ("'205 Patent") 1:31-3:32. The '205 Patent contains ninety-six (96) claims, eight (8) of which are independent (Claims 1, 17, 33, 49, 63, 77, 91, and 93). Disputed claim terms are contained in Claims 17 and 33. These claims are reproduced below, with disputed terms underlined where they appear.

- **Claim 17:** A system, comprising:

  A security policy management server; and

  One or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to:

  Receive a plurality of dynamic security policies from the security policy management server;

  Receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

  Receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

Receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;

Receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

Receive packets associated with a network protected by the packet security gateway; and

Perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation other than forwarding or dropping the packets.

- **Claim 33:** One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:

  Receive a plurality of dynamic security policies form the security policy management server;

  Receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

  Receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

  Receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;

  Receive, a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first

time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

Receive packets associated with a network protected by the packet security gateway; and

Perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

B. The '077 Patent

The '077 Patent was issued on January 31, 2017 and claims an invention entitled "Method and Systems for Protecting a Secured Network." Am. Compl. ¶ 11. The '077 Patent, like the '205 Patent, discloses various methods by which a device within a secured network is programmed to perform protective functions on incoming packets. See Am. Compl., Ex. C ("'077 Patent") at 1:41-3:47. The '077 Patent has twenty (20) claims, five (5) of which are independent (Claims 1, 7, 13, 19, and 20). Disputed terms are contained in claims 7 and 13. These claims are reproduced below, with disputed terms underlined where they appear.

- **Claim 7:** A system comprising:

  At least one processor; and

  A memory storing instructions that when executed by the at least one processor cause the system to:

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

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

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 one or more rules, drop the portion of the packets; and

Modifying a switching matrix of a local area network (LAN) switch associated with the devise such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device.

- **Claim 13:** One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:

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

Configure, 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.

B. The '370 Patent

The '370 Patent was issued on February 16, 2016 and is entitled "Correlating Packets in Communications Networks." Am. Compl. ¶ 9. The '370 Patent relates to correlating packets received by communications networks. The '370 Patent contains two-hundred and five (205)

claims, eighteen (18) of which are independent (Claims 1, 22, 43, 64, 76, 88, 100, 111, 122, 133, 142, 151, 160, 169, 178, 187, 194, and 201). Disputed claim terms are contained in Claims 61 and 43.[2] These claims are reproduced below, with disputed terms underlined where they appear.

- **Claim 61:** The one or more non-transitory computer-readable media of claim 43, wherein the host located in the second network is associated with a malicious entity, and wherein the instructions, when executed by the computing system, cause the computing system to generate data configured to cause the first network to drop packets transmitted by the host located in the first network.

  Claim 43 One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing 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 computing 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 computing system, the plurality of log entries corresponding to the plurality of packets received by the network device;

[2] The parties have agreed that claim 61 is representative of the claims contained in the '370 patent, however claim 61 depends on independent claim 43. Several of the disputed terms are contained in Claim 43, therefore, I have reproduced claim 43 in addition to claim 61.

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 computing 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.

D. The '722 Patent

The '722 Patent was issued on August 9, 2016 for an invention entitled "Rule-Based Network-Threat Detection." See Am. Compl. ¶ 12.

Specifically, the '722 Patent discloses a manner by which a "packet-filtering device" is enabled to perform multiple threat-detection functions, such as receiving and identifying "a packet" that corresponds to specified network-threat indicators, and preventing a packet that so corresponds from continuing forward to its destination. Id. at 1:46-63. The '722 Patent contains twenty-five (25) claims, one (1) of which is independent (Claim 1). All disputed claim terms are

contained in Claims 1 and 25 of the patent. These claims are reproduced below, with disputed terms underlined where they appear.[3]

- **Claim 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

[3] Double underlines are used to denote overlap, i.e. where a word is construed individually, as well as part of a phrase.

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, 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.

- **Claim 25:** The method of claim 1, wherein:

  Receiving a plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices.

E. The '213 Patent

The '213 Patent was issued on February 7, 2017 for an invention entitled "Method and Systems for Protecting a Secured Network." Am. Compl. ¶ 13. Similar to both the '205 and '077 patents, the '213 patent discloses various methods by which a device within a secured network is programmed to perform protective functions on incoming packets. See Am. Compl., Ex. E ("213 Patent") at 1:31-3:37. The '213 Patent has sixteen (16) claims, of which two are independent (Claims 1 and 10). See '213 Patent. Disputed terms are contained in claims 1 and 3 of the '213 Patent. These claims are reproduced below, with disputed terms underlined where they appear.

- **Claim 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.

- **Claim 3:** The method of claim 1, wherein at least one rule indicates performing a deny packet transformation function on the packets comprising the application-layer packet-header information, and wherein performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information.

F. The '856 Patent

The '856 Patent was issued on March 13, 2018 for an invention entitled "Rule-based Network-Threat Detection for Encrypted Communications." Am. Compl. ¶ 14. Aspects of the '856 Patent relate to "rule-based network-threat detection for encrypted communications." See Am. Compl., Ex. F (the "'856 Patent") 1:31-1:32. The '856 Patent has twenty-five (25) claims, three (3) of which are independent (Claims 1, 24 and 25). Id. at 25:13-30:31. Disputed terms are contained in claims 18[4], 24, and 25. These claims are reproduced below, with disputed terms underlined where they appear.

- **Claim 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 the network-threat indicators comprises a domain name identified as a network threat;

  Identifying packets comprising unencrypted data;

[4] The parties have agreed that claim 18 is representative of the claims contained in the '856 patent, however claim 18 depends on independent claim 1. One of the disputed terms is contained in Claim 1, therefore, I have reproduced claim 1 in addition to claims 18, 24, and 25.

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

Filtering, by a 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.

- **Claim 18:** The method of claim 1, wherein:

  The packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:

  Determining that one or more handshake messages comprise the domain name identified as the network threat.

- **Claim 24:** A packet-filtering system comprising:

  At least one hardware processor; and

  Memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

  Receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

  Identify packets comprising unencrypted data;

Identify packets comprising encrypted data;

Determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

Filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, or data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet filtering rules:

Packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

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

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

- **Claim 25:** One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:

Receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

Identify packets comprising unencrypted data;

Identify packets comprising encrypted data;

Determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

Filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, or data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet filtering rules:

Packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

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

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

III. LEGAL PRINCIPLES OF CLAIM CONSTRUCTION

A. General Principles

The purpose of a Markman hearing is to assist the Court in construing the meaning of the patent(s) at issue. Markman v. Westview Instruments, Inc., 517 U.S. 370, 371 (1996); Markman v. Westview Instruments, Inc., 52 F.3d 967 (Fed. Cir. 1995), aff'd, 517 U.S. 370 (1996). Patents consist of "claims," and the construction of those claims "is a question of law, to be determined by the court." Markman, 517 U.S. at 371; Markman, 52 F.3d at 970–71. A court need only construe, however, claims "that are in controversy, and only to the extent necessary to resolve the controversy." Vivid Techs., Inc. v. Am. Science Eng'g, Inc., 200 F.3d 795, 803 (Fed. Cir. 1999) (citations omitted). To be clear, "[c]laim construction is a matter of resolution of disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement. It is not an obligatory

exercise in redundancy." NTP, Inc. v. Research in Motion, Ltd., 418 F.3d 1282, 1311 (Fed. Cir. 2005) (citing U.S. Surgical Corp. v. Ethicon, Inc., 103 F.3d 1554, 1568 (Fed. Cir. 1997)).

Claim construction begins with the words of the claims. Vitronics Corp. v. Conceptromc, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("First, we look to the words of the claims themselves . . . ."). Words in a claim are generally given their ordinary meaning as understood by a person of ordinary skill in the art (a "POSITA"). Id. This "person of ordinary skill in the art is deemed to read the claim term not only in the particular claim in which the disputed term appears but also in the context of the entire patent, including the specification." Phillips v. AWH Corp., 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). "In some cases, . . . the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than application of the widely accepted meaning of commonly understood words." Id. at 1314. Often, however, "determining the ordinary and customary meaning of the claim requires examination of terms that have a particular meaning in a field of art. Because the meaning of a claim term as understood by persons of skill in the art is often not immediately apparent, and because patentees frequently use terms idiosyncratically, the court looks to those sources available to the public that show what a person of skill in the art would have understood disputed claims language to mean." Id.

Further, the claims themselves can provide substantial guidance as to the meaning of particular claim terms. Id. First, "the context in which a term is used within a claim can be highly instructive." Id. In addition, other claims of the patent in question, both asserted and not asserted, can also be useful because claim terms are "normally used consistently throughout the patent" and therefore "can often illuminate the meaning of the same term in other claims." Id.

The claims should not be read alone, however, but rather should be considered within the context of the specification of which they are a part. Markman, 52 F.3d at 978. As the Federal Circuit stated in Vitronics and restated in Phillips, "the specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." Phillips, 415 F.3d at 1315. The Court, however, must not read in limitations from the specification without clear intent to do so. Thorner v. Sony Comp. Entmt. Am. LLC, 669 F.3d 1362, 1366 (Fed. Cir. 2012). Furthermore, a patentee is free to be his or her own lexicographer, and thus if the patentee defines a term in the specification differently than its ordinary meaning, the patentee's definition controls. Phillips, 415 F.3d at 1316.

In addition to consulting the specification, a court may also consider the patent's prosecution history, if in evidence, because it provides information regarding how the United States Patent and Trademark Office and the inventor understood the patent. See id. at 1317. It also enables the Court to determine if the inventor limited the invention during the course of prosecution. Id. "[W]here an applicant whose claim is rejected on reference to a prior patent ... voluntarily restricts himself by an amendment of his claim to a specific structure, having thus narrowed his claim in order to obtain a patent, he may not by construction ... give the claim the larger scope which it might have had without the amendments." I.T.S. Rubber Co. v. Essex Rubber Co., 272 U.S. 429, 444 (1926). Thus, consulting prior art reference in the prosecution history is permissible. Vitronics, 90 F.3d at 1583.

These elements of the patent itself—the claims, the specification, and its prosecution history—constitute intrinsic evidence of claim construction. In addition to such intrinsic evidence, a court may consider extrinsic evidence to determine the meaning of disputed claims. Phillips, 415 F.3d at 1317. Such extrinsic evidence "consists of all evidence external to the

patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises." Phillips, 415 F.3d at 1317 (citing Markman, 52 F.3d at 980). However, the Court should not rely on extrinsic evidence when the intrinsic evidence removes all ambiguity. Vitronics, 90 F.3d at 1583.

Such extrinsic evidence generally is held as less reliable than the intrinsic evidence and "is unlikely to result in a reliable interpretation of patent claim scope unless considered in the context of intrinsic evidence." Id. at 1317–18. With respect to expert evidence, for example, "[c]onclusory, unsupported assertions by experts as to the definition of a claim term are not useful to a court . . . [and] a court should discount any expert testimony that is clearly at odds with the claim construction mandated by the claims themselves, the written description, and the prosecution history, in other words, with the written record of the patent." Id. at 1318.

With respect to general usage dictionaries, the Federal Circuit noted that "[d]ictionaries or comparable sources are often useful to assist in understanding the commonly understood meaning of words and have been used . . . in claim construction," and further noted that "a dictionary definition has the value of being an unbiased source 'accessible to the public in advance of litigation.'" Id. at 1322 (citing Vitronics, 90 F.3d at 1585). However, the Federal Circuit cautions that (1) "'a general-usage dictionary cannot overcome art-specific evidence of the meaning' of a claim term;" that (2) "the use of the dictionary may extend patent protection beyond what should properly be afforded by the inventor's patent;" and that (3) "[t]here is no guarantee that a term is used in the same way in a treatise as it would be by the patentee." Phillips, 415 F.3d 1322 (quoting Vanderlande Indus. Nederland BV v. Int'l Trade Comm'n, 366 F.3d 1311, 1321 (Fed. Cir. 2004)).[5] Indeed, "different dictionary definitions may contain

[5] In Phillips, the Federal Circuit thus expressly discounted the approach taken in Texas Digital Systems, Inc. v. Telegenix, Inc., 308 F. 3d 1193 (Fed. Cir. 2002), in which the court placed greater emphasis on dictionary

somewhat different sets of definitions for the same words. A claim should not rise or fall based upon the preferences of a particular dictionary editor . . . uninformed by the specification, to rely on one dictionary rather than another." Id.

B. The "Canons of Claim Construction"

The Federal Circuit has recognized certain guideposts, or "canons of construction," to assist a district court in determining the meaning of disputed claim terms and phrases. These are merely guideposts, however, and are not immutable rules:[6]

1. Doctrine of Claim Differentiation: Ordinarily, each claim in a patent has a different scope. See, e.g., Versa Corp. v. Ag-Bag Int't Ltd., 392 F.3d 1325, 1330 (Fed. Cir. 2004). Ordinarily, a dependent claim has a narrower scope than the claim from which it depends. See, e.g., Phillips, 415 F.3d at 1315. Ordinarily, an independent claim has a broader scope than a claim that depends from it. See, e.g., Free Motion Fitness, Inc. v. Cybex Int'l, Inc., 423 F.3d 1343, 1351 (Fed. Cir. 2005).

2. Ordinarily, claims are not limited to the preferred embodiment disclosed in the specification. See, e.g., Phillips, 415 F.3d at 1323.

3. Ordinarily, different words in a patent have different meanings. See, e.g., Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1119–20 (Fed. Cir. 2004).

4. Ordinarily, the same word in a patent has the same meaning. See, e.g., Phillips, 415 F.3d at 1314.

5. Ordinarily, the meaning should align with the purpose of the patented invention. See, e.g., Innovad Inc. v. Microsoft Corp., 260 F.3d 1326, 1332–33 (Fed. Cir. 2001).

---

definitions of claim terms. Phillips, 415 F.3d at 1319–24 ("Although the concern expressed by the court in Texas Digital was valid, the methodology it adopted placed too much reliance on extrinsic sources such as dictionaries, treatises, and encyclopedias and too little on intrinsic sources, in particular the specification and prosecution history."). The Federal Circuit reaffirmed the approach in Vitronics, Markman, and Innova as the proper approach for district courts to follow in claim construction, but acknowledged that there was "no magic formula" for claim construction, and that a court is not "barred from considering any particular sources . . . as long as those sources are not used to contradict claim meaning that is unambiguous in light of the intrinsic evidence." Phillips, 415 F.3d at 1324.

[6] This list is derived from the one provided in the FEDERAL JUDICIAL CENTER, PATENT LAW AND PRACTICE § 5.I.A.3.d (5th ed. 2006).

6. Ordinarily, general descriptive terms are given their full meaning. See, e.g., Innova/Pure Water, Inc., 381 F.3d at 1118.

7. If possible, claims should be construed so as to preserve their validity. See, e.g., Energizer Holdings, Inc. v. Int'l Trade Comm'n, 435 F.3d 1366, 1370–71 (Fed. Cir. 2006).

8. Ordinarily, absent broadening language, numerical ranges are construed exactly as written. See, e.g., Jeneric/Pentron, Inc. v. Dillon Co., 205 F.3d 1377, 1381 (Fed. Cir. 2000).

9. Ordinarily, absent recitation of order, steps of a method are not construed to have a particular order. See, e.g., Combined Sys., Inc. v. Def. Tech. Corp. of Am., 350 F.3d 1207, 1211–12 (Fed. Cir. 2003).

10. Absent highly persuasive evidentiary support, a construction should literally read on the preferred embodiment. See, e.g., Cytologix Corp. v. Ventana Med. Sys., Inc., 424 F.3d 1168, 1175 (Fed. Cir. 2005).

IV. DISPUTED TERMS

A. '205 Patent

1. "packet-transformation functions specified by the plurality of dynamic security policies"[7]

After the Court heard argument of counsel, the parties agreed that the proper construction of this term is **"function specified by the dynamic security policy where the dynamic security policy is subject to change."**

2. "rule/rules"[8]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"a condition or set of conditions that when satisfied cause a specific function to occur."**

[7] This phrase combines two previously disputed terms: "packet transformation function/functions" and "dynamic security policy."

[8] Doc. 106 at 8; Doc. 106 at 22; Doc. 117 at 6; Doc. 119 at 18. Affecting claims 17 and 33.

Plaintiff contended that its construction of the term "rule/rules" is consistent with how the term is utilized within the specifications of the patent. Doc. 106 at 8 (citing e.g. '205 Patent, Col. 20:23-27 ("at least one rule specifying that all packets associated with network addresses outside of the set of network addresses"); 21:38-42 ("at least one rule specifying the method comprising routing..."). Additionally, Plaintiff alleged that a person of skill in the art would understand the term "rule" to have the type of "if/then" purpose. Id.

Defendants argued that a "rule" within the context of the asserted claims contains two aspects: criteria and function. See Doc. 104 at 23. Defendants contended that Plaintiff's construction addresses the first aspect "criteria" by indicating that a rule is a set of "conditions" but misses the "function" aspect. Id. However, Defendants reproduced Figure 3 from the '205 Patent and contended that the Figure shows that each of the rules specify not only the criteria for the packets, but also specif[y] the "function" to be performed on the packets. Id.

The Court examined the Plaintiff's construction of the term "rule/rules," and determined that the construction did not seem to be inconsistent with the way that a rule operates within the specification. However, in light of the fact that Figure 3 of the '205 Patent contains the word "function," and Plaintiff could provide no meaningful distinction between the words "function" and "action," the Court adopted Plaintiff's construction and changed the word "action" to "function" in order for the construction to be consistent with the language of the specification.

B. The '077 Patent

1. "rule/rules"[9]

In construing the term "rule/rules" both parties agreed that the term "rule/rules" in the '077 Patent has the same meaning as it does in the '205 Patent, therefore, the Court **RULED** that

[9] Doc. 106 at 9; Doc. 104 at 28; Doc. 117 at 7; Doc. 119 at 28. Affecting claims 7 and 13.

the proper construction of this term is **"a condition or set of conditions that when satisfied cause a specific function to occur."**

2. "switching matrix of local area network (LAN) switch"[10]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"a switching matrix contained within a local area network switch that is configured to direct traffic in a local area network (LAN)."**

Plaintiff contended that a person of skill in the art would understand the term "matrix" to mean "a component that is directing traffic from one device to another in the network." Doc. 106 at 10 (citing Medvidovic Decl. ¶ 19). At the hearing, Plaintiff argued that Defendants' proposed construction, which defined the term "matrix" as a "structure," may confuse the jury into thinking that a "matrix" is a separate structure than the local area network switch.

Defendants agreed that a matrix is not a separate structure than the local area network switch, but averred that the term "matrix" needs to be defined. See Doc. 104 at 29. Additionally, Defendants argued that Plaintiff's construction departs from the words of the claims because the phrase "may be configured" indicates that the configuration of the matrix in such a manner is "a mere option." Id. Defendants alleged that the patent examiner rejected such a broad construction. Id.

Plaintiff also contended that Defendants' construction contained a limitation that the switching matrix only direct traffic "received from one or more devices on a local area network to one or more devices on the local area network" when a switching matrix can also switch packets received from other sources.

[10] Doc. 106 at 10; Doc. 104 at 28; Doc. 117 at 8; Doc. 119 at 28. Affecting claims 17 and 33.

The Court agreed that the language in the claims supports Defendants' contention that that the "switching matrix of a local area network (LAN) switch...is configured to drop the portion of the packets." '077 Patent, Claims 7 and 13. Therefore, the Court rejected Plaintiff's argument that a "switching matrix" may be configured to do something else. The Court also agreed with Plaintiff's argument that embodiment of the invention described within the specification indicated that a "switching matrix" could switch packets received from networks external to the local area network. Therefore, the Court adopted a construction that contained language from both Plaintiff and Defendants' proposed constructions.

C. The '370 Patent

1. "network device"[11]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"a computing device in a network that is capable of transmitting and receiving packets."**

Plaintiff argued that its construction best demonstrates how the term "network device" is construed within the various claims and specifications of the '370 patent. Doc. 106 at 13. Plaintiff alleged that in each usage of the term "network device" the language indicates that a "network device" is capable of "transmitting and receiving packets of data." Id (citing '370 Patent, Claims 22-26, 33, 43-47, 54, 187-188, 191, 194, 198, 201-202, 205 ("plurality of packets received by the network device" and then a "plurality of packets are transmitted by the network device"); '370 Patent, Col. 13:36-14:9 (specification describes a network device as a device that receives and transmits packets).

[11] Doc. 106 at 13; Doc. 104 at 19; Doc. 117 at 12; Doc. 119 at 16. Affecting claim 61 (and incorporated by reference, claim 43).

Defendants contended that a "network device" as used within the patent, always performs the function of "interfac[ing] hosts." Defendants cited language in the specification that defines the function of a "network device" as "one or more devices...that interface host 108, 110, and 112 with network 106. Similarly, network device(s)...may include one or more devices that interface hosts 114, 116, and 118 with network 106." Doc. 104 at 19 (citing '370 Patent, Col. 2:44-52; '370 Patent, Fig. 1). Defendant also claimed that Plaintiff's construction collapses the distinction between "device in a communication link" and the "network device." Doc. 104 at 19-20.

The Court examined language from the specification which indicated that "tap device 126 may have access to a communication path that interfaces network device(s) 122 and host 114." '370 Patent, Col. 3:42-44. From this language, the Court determined that the "communication path" may interface network device(s) and hosts. Therefore, the Court determined that the "network device" is not limited to interfacing hosts, and may also interface "communication paths." Therefore, the Court adopted Plaintiff's construction of the term "network device."

2. "host"[12]

At the hearing, the parties agreed that the proper construction of the term "host" is **"computing or network devices, such as servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, switches, or access points."**

[12] Doc. 106 at 14; Doc. 104 at 20; Doc. 117 at 13; Doc. 119 at 17. Affecting claim 61 (and incorporated by reference, claim 43).

3. "rule/rules"[13]

In construing the term "rule/rules" both parties agreed that the term "rule/rules" in the '370 Patent has the same meaning as it does in the '077 and '205 Patents, therefore, the Court **RULED** that the proper construction of this term is **"a condition or set of conditions that when satisfied cause a specific function to occur."**

4. "log entries"[14]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"notations of identifying information for packets."**

Plaintiff argued that no construction of the term "log entries" is necessary. Plaintiff also contended that Defendants' construction, requiring that the log entries be "unique" for "each packet," unnecessarily adds requirements to the term "log entries" that are not supported by the intrinsic language of the patent. Doc. 106 at 17.

Defendants assert that their construction of the term "log entries" is consistent with the specifications of the patent, and that the term "log entries" is too abstract for a jury to understand its meaning within the scope of the patent. Doc. 104 at 17 (citing Eon Corp. IP Holdings v. Silver Spring Networks, 815 F.3d 1314, 1320 (2016) (finding that district court erred by instructing the jury to give the terms "portable" and "mobile" their plain and ordinary meaning because the term had more than one ordinary meaning and reliance on the ordinary meaning did not resolve the parties' dispute).

The Court **RULED** that the term "log entries" needed to be construed. The Court agreed that the portion of Defendants' proposed construction which indicates that the log entries are

[13] Doc. 106 at 14; Doc. 104 at 14; Doc. 117 at 15; Doc. 119 at 11. Affecting claim 61 (and incorporated by reference, claim 43).

[14] Doc. 106 at 16; Doc. 104 at 16; Doc. 117 at 15; Doc. 119 at 13. Affecting claim 61 (and incorporated by reference, claim 43).

"notations" was consistent with the patent language. However, the Court struck the language to which Plaintiff objected, because the intrinsic language of the patent did not require that the entries be "unique" or that the entries be tied to "each" packet.

5. "correlate/correlating"[15]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"packet correlator may compare data in one or more log entries with data in one or more other log entries to identify the host."**

The parties agreed that the function of "correlating" is performed by a "packet correlator" but their constructions differ in regard to what the act of "correlating" does. Plaintiff argued that a "packet correlator" does correlating and "applies programming instructions" in order to determine whether a portion of data in one log entry corresponds to a portion of data in another log entry. Doc. 106 at 18. Plaintiff contended that Defendants construction imported a limitation that the correlator "log entries to the same single packet," which is not required by the '370 Patent. Id.

Defendants contended that their construction of the term "correlate" to include determining "whether log entries in different files correspond to the same packet" is consistent with the specification. Doc. 104 at 15. Defendants cited a portion of Claim 22 in support of their construction, which states that the claimed correlation is "based on a plurality of log entries corresponding to the plurality of packets transmitted by the network device." Id. Defendants asserted that Plaintiff's construction is improper because the claims do not limit "correlating" to making a determination based on a "portion" of data in a log entry. Doc. 119 at 13.

[15] Doc. 106 at 17; Doc. 104 at 15; Doc. 117 at 16; Doc. 119 at 12. Affecting claim 61 (and incorporated by reference, claim 43).

The Court agreed that Defendants' proposed construction seemed add language to the patent. There is no language in the '370 Patent that supports Defendants' contention that the packet correlator examines "log entries in separate files," nor is the term "files" recited anywhere in the language of the patent. Therefore, the Court adopted portions of Plaintiff's proposed construction, but added language from the specification that Plaintiff cited in order to construe the term "correlate/correlating" in a manner that more closely aligned with the language intrinsic to '370 Patent.

6. "device in a communication link"[16]

After the hearing began, the parties advised the Court that they no longer disputed this term, and that the term would have its plain and ordinary meaning.

7. "configured to cause the system/computing system to log packets"[17]

Plaintiff's Construction	Defendants' Construction
programming instructions that cause the system to generate a log file containing packet data	no construction needed/plain meaning

After considering the claim language and the Parties' arguments, the Court **RULED** that no construction of this term is necessary.

Plaintiff argued that its construction both "gives meaning to [the] term consistent with what the patentee intended to be covered...and its plain and ordinary meaning." Doc. 106 at 22. In support of its construction, Plaintiff cited a portion of the patent's specifications which recites language that "rule(s) 140, which may configure tap device(s) 124 and 125 to identify packets meeting criteria specified y rule(s) 140 and to communicate data associated with the identified

[16] Doc. 106 at 18; Doc. 104 at 18; Doc. 117 at 18; Doc. 119 at 15. Affecting claim 61 (and incorporated by reference, claim 43).
[17] Doc. 106 at 21; Doc. 104 at 19; Doc. 117 at 21; Doc. 119 at 18. Affecting claim 61 (and incorporated by reference, claim 43).

packets...utilize the data to generate one or more log entries corresponding to the identified packets in log(s) 142." Id (citing '370 Patent, Col. 3:13-20).

Defendants argued that no construction of the term "configured to cause the system/computing system to log packets" was necessary and that the term should have its plain and ordinary meaning. Further, Defendant argued that Plaintiff's use of the terminology "generat[ing] a log file" is not consistent with the language of the patent or the specifications because the specifications do not indicate that a "log file" is created. Doc. 104 at 21. Defendants also contend that the patent does not recite any "programming instructions." Id.

The Court agreed with Defendant that no construction of the term is necessary.

D. The '722 Patent

1. "packet-filtering rules"[18]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"condition or set of conditions that when satisfied cause the specific function of packet-filtering to occur."**

Because the Court previously **RULED** that the construction of the term "rules" is "condition or set of conditions that when satisfied cause a specific function to occur," the Court construed the term "packet-filtering rules" by using the previous construction and adding the words "packet-filtering."

2. "interface"[19]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"a display visible to the user that allows a user to provide input."**

[18] Doc. 106 at 24; Doc. 104 at 5; Doc. 117 at 24; Doc. 119 at 4. Affecting claims 1 and 25.
[19] Doc. 106 at 26; Doc. 104 at 11; Doc. 117 at 25; Doc. 119 at 9. Affecting claims 1 and 25.

Plaintiff asserted that the term "interface" requires no construction, because the term "interface" is well understood by one of skill in the art and its meaning is clear within the context of the claims asserted. Doc. 106 at 26. Additionally, Plaintiff contended that Defendants' proposed construction inappropriately requires that the interface be "visible to the user," which imposes a limitation inconsistent with the language in the patent specifications. Id.

Defendants claim that construing the term "interface" to mean "a display visible to the user that allows the user to provide input" is consistent with the language of the specifications. Doc. 104 at 11. Defendants' cited language in claim 1 that states: "causing, by the packet-filtering device and an interface, display of the information." Id. Defendant did not contest that the term "interface" has a different meaning in the language of some of the specifications, but argued that the term "interface" has the meaning that of a "display visible to the user" within the context of Claim 1 of the '722 patent. Doc. 119 at 9 (citing PowerOne, Inc. v. Artesyn Techs., Inc., 599 F.3d 1343, 1348 (Fed. Cir. 2010) ("The terms, as construed by the court, must 'ensure that the jury fully understands the court's claim construction rulings and what the patentee covered by the claims")).

The Court **RULED** that the term "interface" needed to be construed. After examining the language in claim 1, the Court agreed with Defendants' argument that the use of the term "interface" within claim 1 of the '722 Patent is consistent with the construction that it proposes.

3. "operator"[20]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"an instruction that modifies or reconfigures the packet filtering device to either prevent or allow a packet to continue to a destination."**

[20] Doc. 106 at 27; Doc. 104 at 7; Doc. 117 at 25; Doc. 119 at 7. Affecting claims 1 and 25.

Defendants agreed with Plaintiff that the "operator" functions to block or allow packets. Doc. 104 at 7. However, Defendants objected to Plaintiff's use of the word "adjustable" as redundant, because claim 1 expressly requires "modifying...at least one operator." Doc. 104 at 7-8; '722 Patent, Claim 1.

Plaintiff contended that Defendants' argument regarding their use of the word "adjustable" is unwarranted because the fact that an "operator" is adjustable is supported by the claims and the contents of the specification. Id. at 25 (citing '722 Patent, Claim 1 ("modifying, by the packet-filtering device, at least one operator..."); '722 Patent, Col. 2:5-10 ("The interface may comprise an element that when invoked by a user of the user device causes the user device to instruct the packet-filtering device to reconfigure the operator")).

The Court agreed with Defendants that the word "adjustable" does not appear within the language of the patent. Therefore, the Court struck the word "adjustable" from Plaintiff's construction, and added the words "modifies" and "reconfigures" to Plaintiff's construction in order for the language in Plaintiff's proposed construction to be consistent with the language of the patent.

4. "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"[21]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"communicating, by the packet-filtering device, information from the packet-filtering rule that identifies and records 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."**

[21] Doc. 106 at 28; Doc. 104 at 10; Doc. 117 at 27; Doc. 119 at 8. Affecting claims 1 and 25.

Plaintiff alleged that its construction clarifies that the term "communicating" means "the causing of a packet-filtering device to generate and communicate a record of data regarding the first packet." Doc. 106 at 29 (emphasis added). Defendants claimed that no construction of this term is necessary, and that Plaintiff's construction appears to be a "rewrite" that uses language not found in the patent. Doc. 104 at 10. At the hearing, Plaintiff clarified that its main issue with using the language in the claim without any construction is that the language of the claim does not describe the functionality that the packet-filtering device "records" as well as "identifies" data. In support of its argument, Plaintiff cited language from the specifications of the '722 patent, which indicates that a "packet-filtering device may...generate [i.e. record] log data." '722 Patent, Col. 6:13-24.

The Court determined that the phrase "communicating, by the packet filtering device..." in large part did not need construction. However, the Court also agreed that the language of the specification cited by Plaintiff supported a construction that demonstrated the packet-filtering device's capability to "record" data. Therefore, the Court added the language "and records" to the term, in order for the construction of the term to better align with the language cited by Plaintiff.

5. "user"[22]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"human."**

Defendant argued that the term user should be construed as "person (e.g., administrator)" because the language in the claims and specification confirms that a "user" is a human. Doc. 104 at 8 (citing '722 patent, claim 1).

[22] Doc. 104 at 8; Doc. 117 at 29; Doc. 119 at 7. Affecting claims 1 and 25.

Plaintiff argued that the teachings of the specification indicate that the term "user" is not limited to a "person" but is recited as "anything that specifies a time interval, modifies an option, or operates a device." Doc. 117 at 29. Therefore, Plaintiff claimed that either "a person" or "a process" can perform the functions of a "user" within the scope of the patent.

The Court reviewed the language cited in the specification, and **RULED** that the term "user" had the meaning "person" in the specifications. See e.g. '722 Patent, Col. 7:52-53 ("graphical depiction may comprise a line chart depicting, for a user-specified time interval"); 9:33-35 ("Interface 600 may include one or more block options that when invoked by a user of a host 110 (e.g., the administrator of network 102)"). Therefore, the Court adopted Defendants' proposed construction of the term.

E. The '213 Patent

At the hearing, the parties indicated that there are no disputed terms within the '213 patent.

F. The '856 Patent

1. "proxy system"[23]

After considering the claim language and the Parties' arguments, the Court **RULED** that the proper construction of this term is **"a proxy system which intervenes to prevent threats in communications between devices."**

Defendants argued that the term "proxy system" should be construed while Plaintiff argues that the term should be given its "plain meaning." Doc. 240 at 8. Defendants contended that the term "proxy system" requires construction because an ordinary jury is not likely to understand the meaning that a person of ordinary skill in the art would apply to the term. Id. at

[23] Doc. 240 at 5; Doc. 241 at 6. Affecting claims 18, 24, and 25.

5. Defendants alleged that the patent uses the term to refer to a collection of proxy devices that establish connections between devices in trusted and untrusted networks and relay communications between those devices. Id. at 6.

Plaintiff argued that Defendants' proposed construction is likely to confuse rather than clarify the term. Doc. 241 at 4 (citing ActiveVideo Networks, Inc. v. Verizon Communications, Inc., 801 F. Supp.2d 465, 485 (E.D. Va. 2011). Plaintiff also proposed that the ordinary meaning of "proxy system" is an "intermediary system." Doc. 241 at 6. Plaintiff argued that its proposed meaning is supported by the intrinsic record, and that there are no limits within the specifications that require the term "proxy system" to connect only "trusted environments to untrusted environments." Id. at 9. For example, Plaintiff argues that the language of the patent specification indicates that a proxy system can be used to connect a host within same network and with different hosts. Id (citing '856 Patent, Col. 8:6-9).

At the hearing, Defendant argued that its construction appropriately addressed the purpose of "proxy system" within the invention claimed in the '870 patent, which is aimed at threat-detection.

The Court **RULED** that the term "proxy system" should be construed because the meaning of the term is not readily apparent to a lay person. The Court also agreed that the language of the '870 Patent did not limit the function of a "proxy system" solely to connecting trusted environments with untrusted environments. Therefore, the Court adopted a construction that addressed both Plaintiff and Defendants' arguments. The Court's construction aligns with the purpose of a proxy system to act as an "intermediary" or "intervene" for the purpose of "threat detection" between devices.

V. CONCLUSION

For the reasons stated on the record and elaborated in this Opinion and Order, the Court construed the disputed terms as follows:

Disputed Term	The Court's Construction
packet-transformation functions specified by the plurality of dynamic security policies	function specified by the dynamic security policy where the dynamic security policy is subject to change
rule/rules	a condition or set of conditions that when satisfied cause a specific function to occur
switching matrix of local area network (LAN) switch	a switching matrix contained within a local area network switch that is configured to direct traffic in a local area network (LAN)
network device	a computing device in a network that is capable of transmitting and receiving packets
host	computing or network devices, such as servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, switches, or access points
log entries	notations of identifying information for packets
correlate/correlating	packet correlator may compare data in one or more log entries with data in one or more other log entries to identify the host
packet-filtering rules	condition or set of conditions that when satisfied cause the specific function of packet-filtering to occur
interface	a display visible to the user that allows a user to provide input
operator	an instruction that modifies or reconfigures the packet filtering device to either prevent or allow a packet to continue to a destination
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	communicating, by the packet-filtering device, information from the packet-filtering rule that identifies and records 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
user	human

proxy system	a proxy system which intervenes to prevent threats in communications between devices

The Clerk is **REQUESTED** to deliver a copy of this Order to all counsel of record.

It is so **ORDERED.**

/s/
Henry Coke Morgan, Jr.
Senior United States District Judge

HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

Norfolk, VA
~~August~~ Sep 11, 2018