UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

_____

Case No. IPR2018-01512
Patent No. 9,565,213

PATENT OWNER'S RESPONSE
UNDER 37 C.F.R. § 42.120

TABLE OF CONTENTS

Page

I. Introduction....1

II. Facts....4

A. Overview of the '213 Patent....4

B. Challenged Claims....8

III. Claim Construction....8

A. "packet" (all challenged claims)....9

B. "dynamic security policy" (all challenged claims)....12

C. "rule/rules" (all challenged claims)....16

D. "security policy management server" (all challenged claims)....17

E. "packet security gateway" (all challenged claims)....17

F. "packet transformation function" (all challenged claims)....18

G. "monitoring device" (all challenged claims)....18

IV. Public AVAILABILITY of ACNS....19

V. Specific Reasons Why The Cited References Do Not Invalidate The Claims 22

A. ACNS in View of Kjendal Does Not Render Obvious Claims 1–9 ...22

1. Petitioner Has Not Demonstrated that ACNS and Kjendal Disclose Receiving a Dynamic Security Policy From a Security Policy Management Server (Elements [1.1] & [1.2])....22

(a) ACNS Does Not Disclose the Claimed Packet Security Gateway....23

(b) ACNS Does Not Disclose Receiving Dynamic Security Policies....24

(c) ACNS' Policies are Not Dynamic Security Policies 28

2. ACNS and Kjendal Do Not Teach the Claimed Packet Digest Logging Function (Element [1.2]) 31

(a) ACNS Fails to Disclose Logging Packets on a Packet-By-Packet-Basis 31

(b) Petitioner Identified Insufficient Motivation to Combine ACNS with Kjendal.....35

(c) There is no Reason to Modify ACNS with Kjendal 37

3. Petitioner Has Not Demonstrated that ACNS in View of Kjendal Discloses Identifying Packets With Application-Layer Packet-Header Information on a Packet by Packet Basis (Element [1.4]) 41

(a) ACNS Does Not Identify Packets on a Packet-By-Packet Basis.....42

4. ACNS Fails to Teach Identifying a Subset of Information Specified By the Packet Digest Logging Function (Element [1.6]).....46

5. ACNS Fails to Teach Generating a Record for Each Packet Identified as Having Application-Layer Packet-Header Information (Element [1.7]).....50

6. ACNS and Kjendal Do Not Teach Routing the Identified Packets to a Monitoring Device in Response to Performing the Packet Transformation Function (Element [1.9]).....51

B. ACNS in View of Kjendal and DiffServ Does Not Render Obvious Claims 10–16.....53

1. Petitioner Has Not Demonstrated that ACNS in View of Kjendal, and DiffServ Discloses Receiving a Dynamic Security Policy From a Security Policy Management Server (Elements [10.1] & [10.2]).....54

2. Petitioner Has Not Demonstrated that ACNS in View of Kjendal, and DiffServ Discloses Receiving a Dynamic Security

Policy With a Rule That Includes a DSCP Selector as the Packet Identification Criteria (claims 10–16).....54

3. Petitioner Has Not Demonstrated that ACNS in View of Kjendal and Diffserv Discloses Identifying Packets With the Packet-Identification Criteria on a Packet by Packet Basis (claims 10–16).....56

4. Petitioner Has Not Demonstrated that ACNS in View of Kjendal, and DiffServ Discloses "routing… to a monitoring device" (claims 10–16).....57

VI. Objective Indicia of Nonobviousness.....57

A. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others.....59

B. Industry Praise.....65

C. Commercial Success and Licensing.....66

VII. Conclusion.....68

TABLE OF AUTHORITIES

Page(s)

Cases

Acceleration Bay, LLC v. Activision Blizzard Inc.,
908 F.3d 765 (Fed. Cir. 2018) 19

Apple Inc. v. Int'l Trade Comm'n,
725 F.3d 1356 (Fed. Cir. 2013) 58

Bicon, Inc. v. Straumann Co.,
441 F. 3d 945 (Fed. Cir. 2006) 15

Crocs, Inc. v. Int'l Trade Comm'n,
598 F.3d 1294 (Fed. Cir. 2010) 58

In re Cuozzo Speed Techs., LLC,
793 F.3d 1268 (Fed. Cir. 2015) 8

In re Cyclobenzaprine Hydrochloride Extended–Release Capsule Patent Litig.,
676 F.3d 1063 (Fed. Cir. 2012) 58, 59

Dell Inc. v. Acceleron, LLC,
818 F.3d 1293 (Fed. Cir. 2016) 15, 18

GrafTech Int'l Holdings, Inc. v. Laird Techs., Inc.,
652 F. Appx. 973 (Fed. Cir. 2016)) 67

Graham v. John Deere Co.,
383 U.S. 1 (1966).....58

Institut Pasteur & Universite Pierre Et Marie Curie v. Focarino,
738 F.3d 1337 (Fed. Cir. 2013) 59

J.T. Eaton & Co. v. Atl. Paste & Glue Co.,
106 F.3d 1563 (Fed. Cir. 1997) 67

Kinetic Techs., Inc. v. Skyworks Solutions, Inc.,
Case IPR2014-00529, Paper 8 (P.T.A.B. Sept. 23, 2014).....50

Leo Pharm. Prods., Ltd. v. Rea,
726 F.3d 1346 (Fed. Cir. 2013) 58

Minnesota Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.,
976 F.2d 1559 (Fed. Cir. 1992)) 67

Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.,
707 F.2d 1376 (Fed. Cir. 1983) 59

Plantronics, Inc. v. Aliph, Inc.,
724 F.3d 1343 (Fed. Cir. 2013) 58

Rambus Inc. v. Rea,
731 F.3d 1248 (Fed. Cir. 2013) 59

Ruiz v. A.B. Chance Co.,
234 F.3d 654, 660 (Fed. Cir. 2000) 58

Statutes

35 U.S.C. § 103 53

Other Authorities

37 C.F.R. § 42.65 51

37 C.F.R. § 42.100(b) 8

Office Patent Trial Practice Guide, 77 Fed. Reg. 48756 at 48766
(Aug. 14, 2012) 8

TABLE OF ABBREVIATIONS

Description	**Abbreviation**
Cisco Systems, Inc.	"Cisco" or "Petitioner"
Centripetal Networks, Inc.	"Centripetal" or "Patent Owner"
Ex. 1001 – U.S. Patent No. 9,565,213	"the '213 Patent"
Ex. 1004 – Declaration of Dr. Jeffay	"Jeffay Decl."
Ex. 1008 – Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5	"ACNS"
Ex. 1009 – Kjendal et al., U.S. Patent No. 9,172,627	"Kjendal"
Ex. 1011 – An architecture for Differentiated Services	"Diffserv"
"security policy management server"	"SPM"
"packet security gateway"	"PSG"

On August 20, 2018, Cisco Systems, Inc., ("Cisco" or "Petitioner") submitted a Petition to institute *inter partes* review ("IPR") of U.S. Patent No. 9,565,213 (Ex. 1001, "the '213 Patent"), challenging claims 1-16. The Board instituted trial on March 20, 2019. *See* Paper 8 ("Institution Decision"). Centripetal Networks, Inc. ("Centripetal" or "Patent Owner") requests the Board find the challenged claims patentable because Petitioner has not proved by a preponderance of the evidence that any claim of the '213 Patent is unpatentable.

I. INTRODUCTION

The claims of the '213 Patent are generally directed to Patent Owner's solutions for operationalizing cyber threat intelligence ("CTI"). One piece of the puzzle for operationalizing CTI is the '213 Patent's security policy management server ("SPM"), which stores, manages, and provides dynamic security policies to one or more packet security gateways ("PSGs"). These dynamic security policies managed by the SPM are dynamic in that they may be automatically updated and provisioned to the PSGs when new CTI—in the form of network addresses known to be associated with malicious network traffic—is received. As noted in the Objective Indicia section, below, Centripetal solved the elusive problem of how to utilize CTI to proactively protect networks from cyber-attacks. The references cited against the challenged claims are lacking this puzzle piece because they do not disclose an SPM that provides dynamic security policies to PSGs. For

example, while ACNS discloses a device that can manage client content policies on more than one content engine, those policies must be updated manually by a network administrator and cannot, therefore, keep up with the ever-evolving flow of CTI.

Another piece of the puzzle involves the packet filtering technique disclosed in the '213 Patent, which is performed on a "packet-by-packet" basis. This term means that the PSGs of the '213 Patent apply rules of the received dynamic security policies (including those specifying application-packet-header information) to identify packets in real time, as they are being received in-transit by the packet security gateway, one packet at a time. This technique differentiates the PSGs of the '213 Patent from prior art content proxies, such as those disclosed in ACNS, which teaches applying rules to reassembled, at rest, application layer messages rather than in-transit individual packets.

The challenged claims also recite a technique for performing a packet transformation function on the individually identified packets. The packet transformation function involves generating a record of each packet that includes a subset of the packet's information (*i.e.* a packet digest), as specified by a "packet digest logging function," and reformatting the subset of information in accordance with a logging system standard. In contrast, ACNS only performs transaction

logging, which involves generating a record on a transaction-by-transaction basis instead of on a packet-by-packet basis.

Compounding these issues, a person having ordinary skill in the art ("POSA") would not have been motivated to combine ACNS with Kjendal and/or Diffserv because ACNS is concerned with analyzing at rest content (e.g., reassembled application layer messages) and not in-transit network traffic flow techniques taught by Kjendal and Diffserv.

Finally, with regard to independent claim 10, the cited references also fail to disclose identifying and performing a packet transformation function on packets that include a Differentiated Service Code Point (DSCP) selector, as recited in independent claim 10. As stated above, ACNS never applies a security policy on individual in-transit packets. Indeed, the combination of Kjendal and DiffServ fails to describe a packet transformation function that is performed on packets corresponding to the DSCP selector.

For at least the foregoing reasons, and the arguments presented below, Patent Owner requests that the Board confirm the patentability of the challenged claims.

II. FACTS

A. Overview of the '213 Patent

U.S. Patent No. 9,565,213 discloses "methods and systems for protecting a secured network." '213 Patent at Title. The '213 patent generally describes a network environment 100, which includes Networks A–E 102, 104, 106, 108, and 110. *Id*. at 4:27–30. Network environment 100 may include packet security gateways ("PSGs") 112, 114, 116, and 118, which receive packets and perform packet transformation functions on the received packets. *Id*. at 4:48–50; 4:66–5:3. Security policy management server ("SPM") 120 may communicate dynamic security policies to the packet security gateways. *Id*. at 4:53–55; 4:66–5:3.

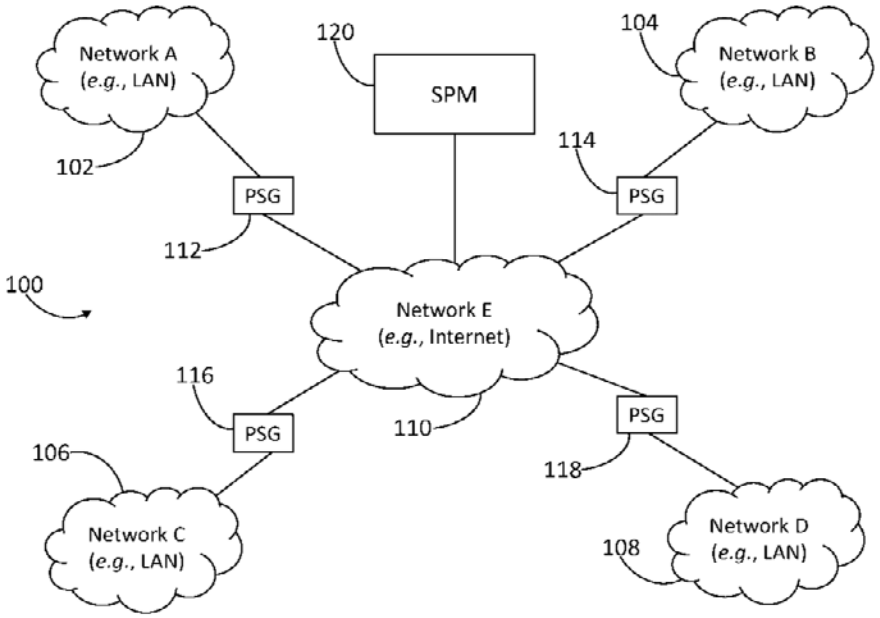


FIG. 1

Id. at Fig. 1.

The exemplary PSGs described in the '213 Patent perform packet transformation functions on the in-transit packets (i.e., as packets are being received), on a packet-by-packet basis, as specified by the dynamic security policy received from the SPM. *Id*. at 5:21–28. A dynamic security policy may include a number of rules that "may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria." *Id*. at 7:10–13. "Rules may specify criteria comprising values selected from five-tuple header information and/or values selected from application-layer header information." *Id*. at 7:67–8:3.

Because the packet identification criteria can include IP packet header and application-layer packet-header information, the PSG is able to filter L2 or L3 (IP) packets on a packet-by-packet basis while the packets are in-transit. Declaration of Dr. Michael Goodrich (Ex. 2004, "Goodrich Decl."), ¶ 51. Indeed, as described in the specification, rather than reassembling application-layer messages, packet filtering rules inspect the application-layer packet-header information located in the HTTP packet portion of an IP packet:

> A rule may specify that **IP packets** containing HTTP packets with a GET method and transferring a resource with a particular URI should have an accept packet transformation function performed on them. Another rule may specify that **IP packets** containing HTTP packets with a PUT method and transferring a resource to a server with a

> particular URI should have a deny packet transformation function performed on them. Rules may specify criteria comprising values selected from five-tuple header information and/or values selected from application-layer header information

'213 Patent at 7:60–8:3. Application-layer packet-header information is structured into standardized fields at specific locations of an IP packet. Because of this feature of application-layer packet-header information, and the fact that these headers are located at the beginning of an application-layer message, the PSGs of the '213 Patent can evaluate the header information at the network level without requiring packet reassembly techniques typically required for application-layer content analysis. Goodrich Decl., ¶ 51.

For example, ACNS does not disclose identifying in-transit packets, on a **packet-by-packet basis,** that include the application-layer packet-header information because ACNS collects and reassembles streams of TCP packets prior to performing their application-layer pattern matching techniques. *Id.* at ¶ 73. Indeed, ACNS performs analysis on at-rest web objects (i.e. content analysis). It does not perform an analysis on individual in-transit packets.

Content analysis of the type disclosed in ACNS is computationally expensive and requires enormous numbers of patterns to account for the proliferation of potential malware attacks. Furthermore, ACNS content analysis is limited to the analysis of HTTP request and response messages, such analysis

requiring the reassembly of the packets that make up the request or response. Conversely, by specifying packet filtering rules based on five-tuple and application-layer packet-header information to be applied to packets, the methods of the '213 Patent can protect a network with huge numbers of computationally inexpensive rules (*e.g.*, as compared to traditional pattern-matching rules applied to reconstructed application-layer messages), thereby permitting proactive network protection that scales to the volume of traffic processed by modern networks. Goodrich Decl., ¶ 53.

Upon matching a rule's criteria, the "rules may further specify a packet transformation function that, when applied to a packet that matches such a rule, produces a digest version, or log, of the packet. This packet log (or digest) may contain selected packet information and/or system information (e.g., associated network addresses, ports, protocol types, URIs, arrival times, packet sizes, directions, interface names, media access control (MAC) addresses, matching rule IDs, metadata associated with matching rules, enforced policy names, or the like)." '213 Patent at 11:46–54. The packet logs may be used by "[a]wareness application servers [that] may read packet logs and perform various transformations on the logs to produce awareness information, which may be accessed by client applications." *Id.* at 11:57–60.

A PSG may also perform "a packet transformation function configured to route or switch packets… to a network address corresponding to a monitoring device." *Id.* at 11:15–19. In order to effectuate this routing, one embodiment of the '213 Patent provides that "the packet transformation function may be configured to encapsulate such packets (e.g., as described by Internet Engineering Task Force (IETF) Request For Comment (RFC) 2003) with an IP header specifying a network address different from their respective destination addresses." *Id.* at 10:49-53. Importantly, the '213 Patent recites that packets are routed to the monitoring device in response to performing a packet digest logging function rather than simply routing packets based on the packet including some particular information. *Id.* at 25:51-55.

B. Challenged Claims

Petitioner challenges claims 1-16 of the '213 Patent, of which claims 1 and 10 are independent.

III. CLAIM CONSTRUCTION

In this *inter partes* review proceeding, "[a] claim in an unexpired patent that will not expire before a final written decision is issued shall be given its broadest reasonable construction in light of the specification of the patent in which it appears." 37 C.F.R. § 42.100(b); *see also* Office Patent Trial Practice Guide ("Trial Practice Guide"), 77 Fed. Reg. 48756 at 48766 (Aug. 14, 2012); *In re*

Cuozzo Speed Techs., LLC, 793 F.3d 1268, 1278 (Fed. Cir. 2015) ("We conclude that Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA.").

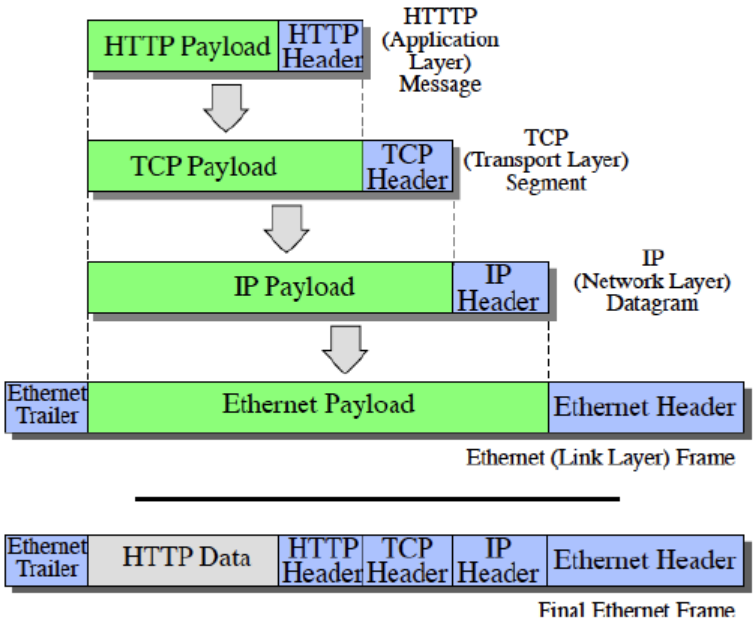
A. "packet" (all challenged claims)

In the context of the '213 Patent, the term "packet" in the '213 Patent refers to a link layer (L2) or network layer (L3) packet of the OSI Model.

As Petitioner's expert, Dr. Jeffay states, "networking professionals… frequently use the generic term 'packet' to refer to one or more transmission units within the protocol stack" and "[g]iven this informal use of the word 'packet,' one must always use the context in which the word appears to understand exactly which type of transmission unit is being referred to." Jeffay Decl., ¶ 53. During his deposition in IPR2018-01386, which also involves the ′213 Patent, Dr. Jeffay testified that the term "packet" used in the claims of the '213 Patent may refer either to link layer packets or network layer packets, but not application layer packets. *See* Dr. Jeffay April 18, 2019 Deposition regarding IPR2018-01386 ("Ex. 2009") at 44:7-46:8, 46:10–47:19 (confirming the term "packet" does not refer to application layer packets because they cannot be received at the packet security gateway but that the received packets could be either link layer or network layer packets). Further, Dr. Jeffay agreed that there is only "one conception of a packet in the claim." *Id.* at 47:12–19. It is apparent then that the packets received by the

packet security gateway and the packets identified, "on a packet-by-packet basis" as including "the application-layer packet-header information" are not application-layer packets.

Dr. Goodrich confirms that the term "packets" as used in the challenged claims refers either to link layer (L2) packets or network layer (L3) packets. Goodrich Decl., ¶ 54. Dr. Jeffay's diagram depicting the "[e]mbedding of protocol data units during the transmission process" is reproduced below for reference:



Jeffay Decl., ¶ 51. The intrinsic record of the 213 Patent fully supports the parties' experts' agreed-upon conception of the term "packet."

First, the '213 Patent discloses two different embodiments regarding how traffic can arrive at the packet security gateway. In one embodiment, the packet security gateway is implemented in a network-layer transparent manner in which

"the packet security gateway may send and receive traffic at a link layer using an interface that is not addressed at the network layer and simultaneously perform the packet transformation function at the network layer." '213 Patent at 3:4–9. One reason for implementing a PSG in a network-layer transparent manner is to "insulate itself from network attacks (e.g., DDoS attacks) launched at the network layer." *Id.* at 6:42–46. In the second embodiment, the packet security gateway alternatively includes a network interface having a network layer address. *Id.* at 3:10–13. In this embodiment, the PSG is network-layer addressable and receives network-layer packets. Accordingly, the packet security gateway may receive "packets" at the link-layer or network-layer. Goodrich Decl., ¶¶ 126-128. Dr. Jeffay's deposition testimony confirms this understanding. *See* Ex. 2009 (April 18, 2019 Jeffay Tr.) at 44:7-46:8; *id*. at 46:14-47:5, 47:7–11 (acknowledging that the packets received at the claimed packet security gateway could be either link layer or network layer packets).

Second, the '213 Patent explicitly states that packet transformation functions operate at the network layer even when the packet security gateway operates in a network-layer transparent manner. '213 Patent at 6:38-41 ("Because packet filter 214 and packet transformation functions 1-N 216, 218, and 220 operate at the network layer, PSG 112 may still perform packet transformation functions at the network layer."). Accordingly, where the claims of the '213 Patent recite

"performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function" (claim 1) or "the packet digest logging function," that language refers to performing packet transformation functions on network layer packets at the network layer. Goodrich Decl., ¶¶ 50-51 (citing '213 Patent, claim 1).

Third, the challenged claims recite "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device." *See* '213 Patent at claims 1 and 10. Petitioner's own expert Dr. Jeffay explains, "'[r]outing' is a specific term in the networking arts and refers to the process that is used by a layer-3 network interconnection device (a router) to transmit a datagram to (or towards) its destination." Jeffay Decl., ¶ 40. Because the claimed PSG is configured to "route" packets, it is apparent that the term "packets" used in the '213 Patent does not refer to application layer messages.

Accordingly, the term "packet" in the '213 Patent based on the OSI Model refers to a L2 or L3 packet.

B. "dynamic security policy" (all challenged claims)

The term "dynamic security policy" means "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets." Petitioner notes that Patent Owner proposed this construction in *Centripetal Networks, Inc., v. Keysight Techs., Inc., et al.*, No. 2:17-cv-

00383/HCM-LRL (E.D. Va.) ("the *Keysight* litigation"). *See* Petition at 14 (citing Ex. 1005, Ex. 1006, and Ex. 1007); *see also* Ex. 2002 (Amended Joint Claim Construction Statement) at 4–5.

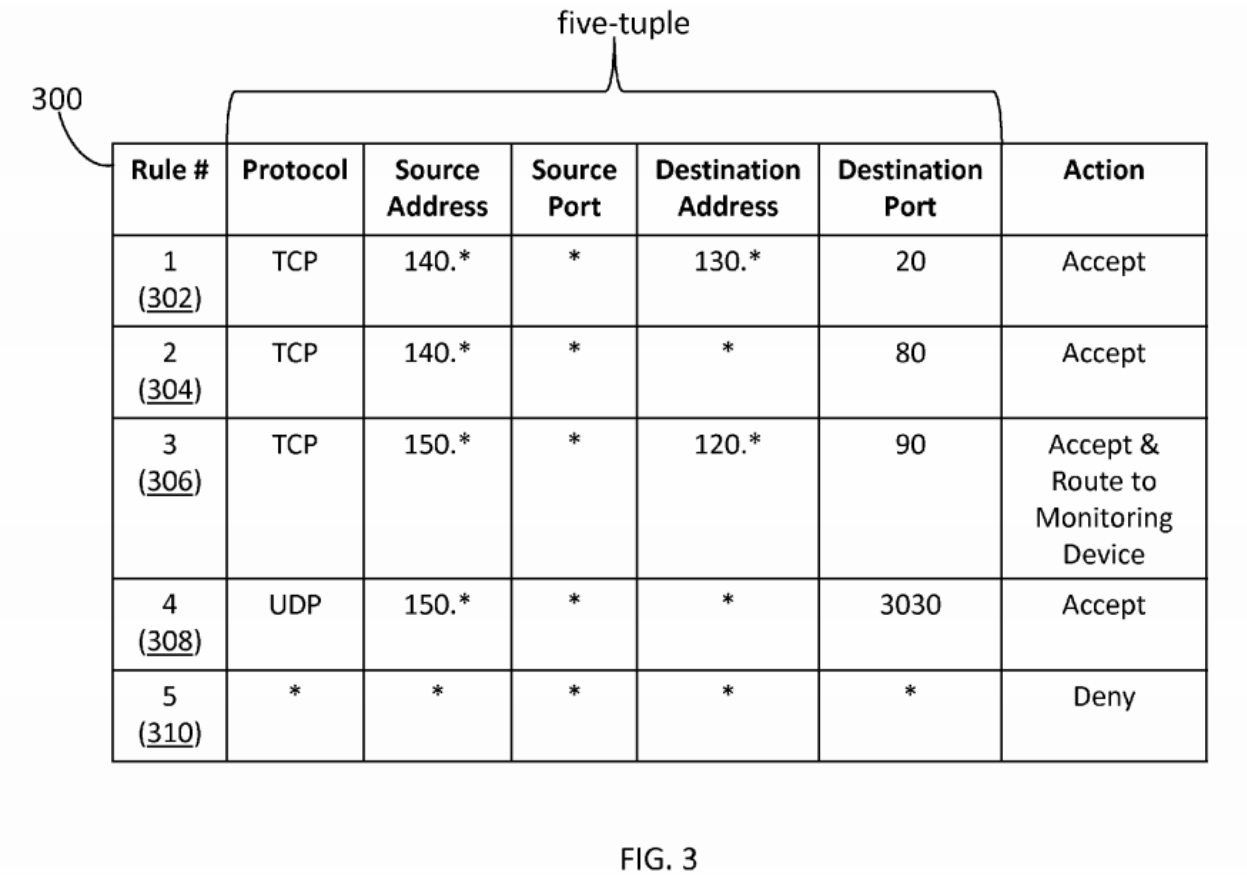
In its Institution Decision, the Board preliminarily construed the term "'dynamic security policy' **to mean** *any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria*." Institution Decision at 9 (italics original) (emphasis added). The Board's preliminary construction is incorrect at least because it improperly conflates the dynamic security policy with elements that may be included therein. Indeed, the Board's construction alters the explicit language used in the specification, which states that a "dynamic security policy **includes** any rule, message," etc. '213 Patent at 4:58–63 (emphasis added). It also differs from the construction proposed by both parties.

The explicit language of the claims confirms the understanding that a rule is not itself a dynamic security policy but may be part of a dynamic security policy. *See* '213 Patent, claim 1 (reciting "a dynamic security policy that comprises at least one rule"). The Board's preliminary construction of the term "dynamic security policy" would transform the claim language into the following phrase, which suggests that the claims require receiving a rule that includes a rule:

> receiving… [**any rule**, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria] **that comprises at least one rule** specifying application-layer packet-header information and a packet transformation function…

'213 Patent, claim 1 (emphasis added).

Patent Owner's proposed construction "a non-static **set** of one or more rules, messages, instructions, files, or data structures associated with one or more packets" captures the relationship between the "dynamic security policy" and what it can "include." For example, the exemplary dynamic security policy disclosed in FIG. 3 of the '213 Patent illustrates that the "dynamic security policy 300 may **include** rules 1-5…." '213 Patent at 7:9–10 (emphasis added).



Rule #	Protocol	Source Address	Source Port	Destination Address	Destination Port	Action
1 (302)	TCP	140.*	*	130.*	20	Accept
2 (304)	TCP	140.*	*	*	80	Accept
3 (306)	TCP	150.*	*	120.*	90	Accept & Route to Monitoring Device
4 (308)	UDP	150.*	*	*	3030	Accept
5 (310)	*	*	*	*	*	Deny

FIG. 3

Id. at FIG. 3.

The Board's preliminary construction also improperly removes any patentable weight from the word "dynamic" in the term "dynamic security policy" and therefore "runs counter to the claim-construction principle that meaning should be given to all of a claim's terms." *Dell Inc. v. Acceleron, LLC*, 818 F.3d 1293, 1300 (Fed. Cir. 2016) (citing *Bicon, Inc. v. Straumann Co.*, 441 F. 3d 945, 950 (Fed. Cir. 2006) ("[C]laims are interpreted with an eye toward giving effect to all terms in the claim.")). In the context of the '213 Patent, the term dynamic means that the security policy can be automatically changed or altered and is, therefore,

"non-static." *See, e.g.*, '213 Patent at 14:19–22 (describing that a security policy management server can communicate a dynamic security policy to a packet security gateway when the dynamic security policy is changed or altered automatically); *see also id*. at 14:48–15:37 (describing a number of circumstances in which a security policy management server may "add, remove, or alter one or more dynamic security policies stored in memory").

Accordingly, the Board should construe the term "dynamic security policy" to mean "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets."

C. "rule/rules" (all challenged claims)

The term "rule/rules" means "a condition or set of conditions that when satisfied cause a specific function to occur." This construction matches the district court's construction of the term in the *Keysight* litigation for Centripetal's U.S. Patent No. 9,137,205 (the "'205 Patent"). Ex. 2001 at 21–22.

In its Institution Decision, the Board adopted Patent Owner's proposed construction. Institution Decision at 9–10. However, the Board also indicated that there was a question as to whether (1) the dynamic security policy includes (i) a rule specifying criteria and (ii) a packet transformation function or (2) that the dynamic security policy includes rules specifying both the criteria and the packet transformation function. *Id.* at 10. The latter understanding comports with the

context provided by the claim language, which specifies that the packet digest logging function is "performed on packets comprising **the** application-layer-packet-header information" specified by the rule. This understanding also comports with the Board's construction of the term rule by providing both the condition or set of conditions (*i.e.* application-layer packet-header information) and the specific function (*i.e.* the packet transformation function comprising the packet digest logging function).

D. "security policy management server" (all challenged claims)

In its Institution Decision, the Board found that the term "security policy management server" means "a server configured to communicate a dynamic security policy to a packet [security] gateway." Institution Decision at 10-11. Without waiving any rights to contest the construction in a District Court litigation, Patent Owner applies this construction herein.

E. "packet security gateway" (all challenged claims)

In its Institution Decision, the Board found that the term "packet security gateway" means "a gateway computer configured to receive packets and perform a packet transformation function on the packets." Institution Decision at 11. Without waiving any rights to contest the construction in a District Court litigation, Patent Owner applies this construction herein.

F. "packet transformation function" (all challenged claims)

In its Institution Decision, the Board construed the term "packet transformation function" to mean "operations performed on a packet." Institution Decision at 13. Patent Owner disagrees and maintains that the proper construction is a "function that transforms one or more packets from one state to another." *Id.* at 11-12. However, Patent Owner applies the Board's preliminary construction herein without waiving any rights to contest the construction in a District Court litigation, as the claims remain patentable under a proper application of the Board's construction.

G. "monitoring device" (all challenged claims)

The term "monitoring device" should be accorded its plain and ordinary meaning, which is "a device configured to monitor packets." The Board's preliminary construction of the term, a "device configured to copy (or store) packets or data contained within them" is incorrect at least because it fails to give patentable weight to the term "monitoring." *Dell*, 818 F. 3d at 1300; Institution Decision at 14-15.

The Board's construction of the term is based on the following disclosure of the '213 Patent:

> The packets may then be routed (or rerouted) to the monitoring device, which may be configured to copy the packets or data contained within them (e.g., for subsequent review by a law enforcement or national

> security authority), strip the IP header from them, and then forward the packets to their destination address (e.g., the address corresponding to the called party or softswitch associated with the called party).

'213 Patent at 11:26-33; Petition at 17; *see also* Institution Decision at 14 (citing '213 Patent at 17:9-18). Given this disclosure, it is apparent that Petitioner's proposed construction adds limitations from an embodiment (*i.e.* that the monitoring device "**may** be configured to copy the packets or data contained within them") while stripping any patentable weight from the term "monitoring."

The construction should therefore be rejected in favor of the plain and ordinary meaning of the term, which is "a device configured to monitor packets."

IV. PUBLIC AVAILABILITY OF ACNS

Petitioner has failed to show that ACNS is a printed publication. *Inter partes* review may only be requested based on prior art that consist of patents or printed publications that were publicly available. 35 U.S.C. § 311(b). To determine whether a reference is deemed a "printed publication," the reference must be publicly accessible. A reference is considered publicly accessible only if it was "disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (citations omitted). As detailed below, Petitioner fails to meet its burden of demonstrating that ACNS is a printed publication.

Petitioner submitted a declaration from Eli Fuchs to establish the public availability of ACNS prior to the filing date of '213 Patent because ACNS (Ex. 1008) does not include a publication date. Mr. Fuchs', however, provides no evidence that ACNS was available prior to the filing date of the '213 Patent and his declaration should not be entitled to any weight for that reason. *See generally* Ex. 1012; Ex. 2021 (Fuchs Tr.) at 40:12-15 (Q. So the evidence -- the only evidence you provide in your declaration would be [Ex. 1008 - ACNS]; is that correct? And your testimony? A. Yes.).

Indeed, Mr. Fuchs' declaration and deposition testimony that ACNS was available "at least as early as March 2008" is solely based on a Google search performed by Mr. Fuchs in preparation for this IPR proceeding. Ex. 1012, ¶ 10. When deposed, Mr. Fuchs stated that he did not know when Ex. 1008 was published and that he formed his opinion on the earliest date Ex. 1008 was published based on a Google search. However, Mr. Fuchs did not provide as evidence of the results of the Google search that he allegedly relied upon to form his opinion. Mr. Fuchs states of his opinion:

> Q. So my question is when was it -- when was the release 5.5 user guide first available to customers?
>
> A. According to this declaration, it was at least by 2008.
>
> Q. And how do you know that it was at least by 2008?

A. I generally recall that when I Googled ACNS 5.5 documentation, the Cisco website had the documentation with the date associated with it, which led me to this declaration about a year ago.

Q. Do you have any other basis for your opinion of when the ACNS version 5.5 guide was first available other than when you did this Google search for it?

A. Not for the date because it was a long time ago.

I do know that it's general practice at Cisco that in order to release a product, you have to release the documentation with it. But I have no memory to recall exact dates. Only by Google research.

Ex. 2021 at 24:20-25:19.

Additionally, the ACNS Guide (Ex. 1008) does not appear to be publically available on the Cisco website currently. As Dr. Goodrich explains, he searched the Cisco website on www.cisco.com on July 3, 2019, and was able to locate the documentation for Cisco ANCS Software Version 5.5.[1] *See* Goodrich Decl., ¶ 63. While he was able to locate the documentation page for the Cisco ACNS Software Configuration Guide for Centrally managed Deployments, Release 5.5, the link that should have taken him to the Ex. 1008 instead redirected to an End-of-Life

[1] Ex. 2017, https://www.cisco.com/c/en/us/support/application-networking-services/acns-software-version-5-5/model.html

retirement notification.[2] *Id.* Accordingly, Dr. Goodrich was not able to access Ex. 1008 as of July 3, 2019. *Id.* Accordingly, there is no evidence that ACNS was publically available as of the filing date of the '213 Patent.

Therefore, Petition lacks sufficient evidence to prove that ACNS was publicly accessible before the critical date.

V. SPECIFIC REASONS WHY THE CITED REFERENCES DO NOT INVALIDATE THE CLAIMS

Claims 1–9 of the '213 Patent are not obvious over ACNS in view of Kjendal, and claims 10–16 are not obvious over ACNS in view of DiffServ in further view of Kjendal.

A. ACNS in View of Kjendal Does Not Render Obvious Claims 1–9

1. Petitioner Has Not Demonstrated that ACNS and Kjendal Disclose Receiving a Dynamic Security Policy From a Security Policy Management Server (Elements [1.1] & [1.2])

ACNS and Kjendal fail to disclose "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," as recited in independent claim 1. As a preliminary matter, Petitioner does not assert that Kjendal discloses a dynamic security policy. *See* Petition at 25-30. Rather,

[2] Ex. 2018, https://www.cisco.com/c/en/us/obsolete/application-networking-services/cisco-acns-software-version-5-5.html

Petitioner cites Kjendal for allegedly describing "a system where application-layer packet-header information is used to determine what should be logged." Institution Decision at 23; Petition at 30-31.

(a) ACNS Does Not Disclose the Claimed Packet Security Gateway

Petitioner asserts that ACNS' Content Engine represents the claimed packet security gateway. However, the Content Engine cannot be a packet security gateway because the Content Engine does not inspect packets and does not perform any security analysis on packet. Eli Fuchs was the Senior Engineering Manager at Cisco that led the software development team responsible for ACNS. Ex. 1012, ¶ 3. Mr. Fuchs submitted a declaration in this case regarding the public availability of ACNS. *Id.*, *generally*. Mr. Fuchs testified during his deposition that the Content Engine does not inspect packets and is not concerned with security:

> Q. Does the content engine perform any security analysis on the request?
>
> A. The content engine does not perform any inspection of data within the object, no.
>
> Q. To be specific, though, does it perform any security analysis on the request itself?
>
> A. It does not.
>
> Q. Does it look at individual packets within the request?
>
> A. It does not.

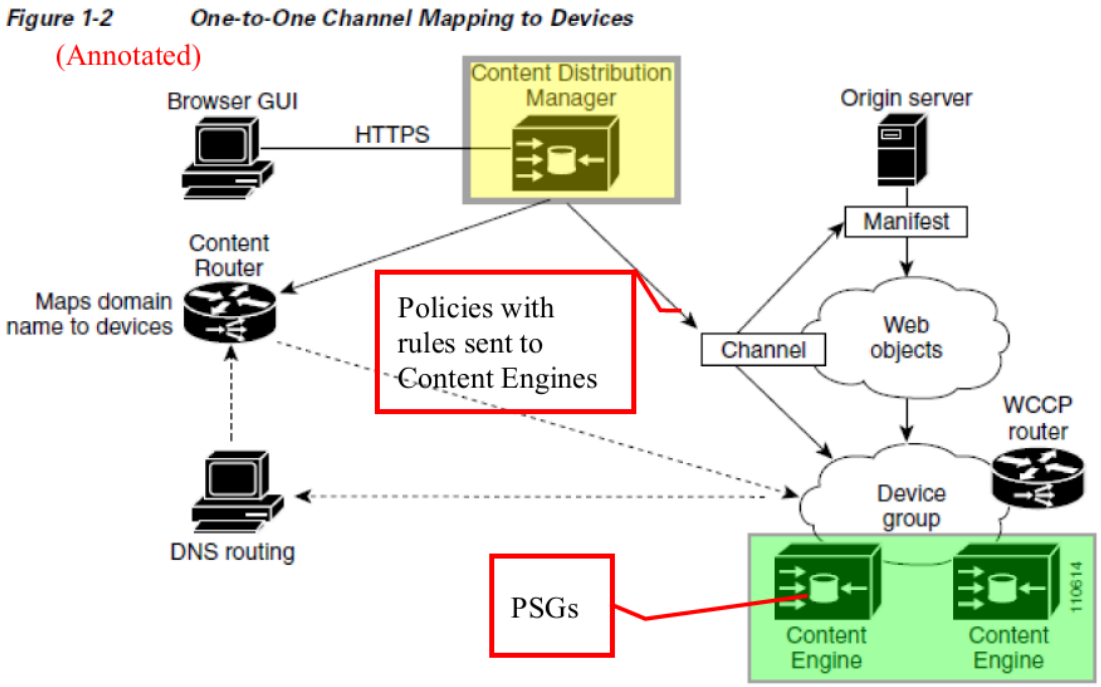
Ex. 2021 (Fuchs Tr.) at 15:2-19.

Moreover, Cisco's own expert witness, Dr. Jeffay confirmed that the Content Engines are not capable of inspecting the payload of a packet for malware. Ex. 2020 (6/5/2019 Jeffay Tr.) at 68:8-69:16. Accordingly, the Content Engine is not the claimed "**packet security** gateway."

(b) ACNS Does Not Disclose Receiving Dynamic Security Policies

ACNS fails to disclose **receiving** dynamic security policies from a security policy management server at each of a plurality of packet security gateways. Rather than transferring the **policies** enforced at each Content Engine, ACNS merely discloses that a user may add to or otherwise modify a policy already existing on a Content Engine. Goodrich Decl., ¶¶ 108-114.

With reference to its annotated version of ACNS Fig. 1-2, Petitioner asserts that ACNS' "Content Engines (marked in green, below) represent the claimed PSGs and are associated with a Content Distribution Manager (CDM, marked in yellow) that represents the claimed SPM Server." Petition at 26.



EX1008, Fig. 1-2 at page 1-11 (annotated).

Id. Further, Petitioner states that ACNS teaches a "dynamic security policy" in the form of "the set of rules used to configure the operation of the Content Engines." Petition at 27.

Petitioner does not cite any evidence to substantiate its claim that ACNS' purported "dynamic security policy" is received at any Content Engine from a Content Distribution Manager. *See id.* ("The dynamic security policy is generated at the CDM based on input by a user…. The policy is then provisioned to one or more Content Engines by the CDM, as shown above in Figure 1-2 of ACNS."). In fact, Petitioner acknowledges that the command-line interface of the Content Distribution Manager is used "for creating and modifying **parts** of a policy." *Id.*

(emphasis added). As explained below, the two examples cited in the Petition clarify that ACNS' Content Distribution Manager does **not** send policies to a Content Engine but is used instead to directly alter a policy already being enforced thereon.

Petitioner first points to a portion of ACNS that involves using the CDM to add a rule to or modify a rule of an existing Content Engine policy. *See* Petition at 27 (citing EX1004, ¶ 153; Ex. 1008 at 8-24). This section of ACNS discloses "Adding or Modifying Additional HTTP Request Methods for the Content Engine." Ex. 1008 at 341 (8-23). Adding or modifying a request method involves manually adding one HTTP request method to a plurality of request methods **already configured** on the Content Engine or modifying one of those **already configured** request methods. *See id.* at 342 (8-24) ("Step 6: In the Method Name field, enter the name of the HTTP request method to be added to the list of supported methods.").

As shown in the step-by-step guide for adding HTTP request methods, if an administrator wants to add an HTTP request method, it must manually add each method to the existing policy implemented on the Content Engine. *See* Ex. 1008 at 342 (8-24); Goodrich Decl., ¶¶ 109-114. That is, ACNS gives a network administrator the ability to manually update an already implemented policy on a Content Engine, but ACNS does not teach that the Content Engines receive their

policies (let alone any dynamic security policies) from a Content Distribution Manager or any other source. *See* Goodrich Decl., ¶¶ 109-114. Accordingly, Petitioner's claim that ACNS discloses "step-by-step instructions for **generating** . . . a policy" on the CDM is contradicted by the record evidence. Petition at 27 (emphasis added).

The Petition's second example of receiving a dynamic security policy using ACNS's command-line interface fails for the same reasons. *See* Petition at 27 (citing ACNS at C-1 – C-27); Goodrich Decl., ¶¶ 111-114. In fact, ACNS' command-line interface simply provide the user an alternative method implementing same functionality provided by the Content Distribution Manager's GUI:

> Table C-1 **maps ACNS software CLI commands to the corresponding Content Distribution Manager GUI procedure**. Software CLI commands are listed in alphabetical order in the first column. The second column indicates the GUI navigation path to the device group configuration window for each command. The third column provides a link to the GUI configuration procedure found elsewhere in this guide.

Ex. 1008 at 895 (C-1) (emphasis added).

Thus, while Petitioner relies upon Table C-1 as allegedly teaching the dynamic security policy provisioned to the Content Engine by the Content Distribution Manager, the Table C-1 only shows a table of commands that may be

manually entered through the CLI to **modify** a setting or rule on the Content Engine. Petition at 27; Ex. 1008 at 895-920 (C-1 – C-26). For example, while Petitioner points to the "http add-method" as allegedly being an example of a "dynamic security policy… generated at the CDM based on input by a user," that command-line command functions exactly the same as the "Adding or Modifying Additional HTTP Request Methods for the Content Engine" cited as Petitioner's first example:

http add-method *method*	Devices > Device Groups > Applications > Web > HTTP > HTTP Method	Adding or Modifying Additional HTTP Request Methods for the Content Engine, page 8-23

Ex. 1008 at 900 (C-6).

In both of these examples, the changes to the already installed policies are static, in that they will be not updated or change automatically as both Dr. Jeffay and the specification agree is required to be dynamic, and do not involve the receipt of a dynamic security policy at a packet security gateway from a security policy management server. *See* '213 Patent at 14:56–59; *see also* Jeffay Decl., ¶ 106 (stating that "dynamically" means "automatically"). Indeed, ACNS does not teach or suggest automatically updating any settings and thus cannot teach or suggest a "dynamic security policy."

(c) ACNS' Policies are Not Dynamic Security Policies

Petitioner's argument that ACNS teaches "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," further relies on its overbroad construction of the term "dynamic security policy," which strips any patentable weight from the word "dynamic." *See* § III.B, *supra*.

As disclosed in the '213 Patent, the security policy management server "may be configured to **add, remove, or alter** one or more dynamic security policies stored in memory 502 based on information received from one or more devices within network environment 100." '213 Patent at 14:48–52 (emphasis added); *see also id.* at 14:13–22 (disclosing a SPM communicating a dynamic security policy to a PSG when the dynamic security policy is "**changed or altered**") (emphasis added). Importantly, the '213 Patent discloses that a **dynamic** security policy can "automatically create or alter one or more of such rules as new network addresses associated with malicious network traffic are determined." *Id.* at 14:56–59. In fact, although Dr. Jeffay opines that in his view "a dynamic security policy is not limited to a 'non-static' set of rules," he does confirm that the distinction between the terms "dynamic" and "static" relates to whether the rules of the security policy are updated automatically or manually. Jeffay Decl., ¶ 106 ("In my opinion, in the context of the '213 Patent, a dynamic security policy is not limited to a 'non-static' set of rules and may be updated dynamically (e.g., automatically) or statically (e.g., manually).").

Petitioner points to ACNS' disclosure of "the set of rules used to configure the operation of the Content Engines" as "dynamic security polic[ies]." Petition at 27. However, the alleged "set of rules" used by the Content Engine is not a "dynamic security policy" because the rules must be manually added or modified by a user operating a GUI or a command line interface (CLI). *See* Ex. 1008 at 341-342 (8-23 – 8-24), 895-920 (C-1 – C-26) (describing static settings that can only be updated, altered, or edited manually by a human network administrator); Goodrich Decl., ¶¶ 111-114. The manually entered settings taught by ACNS cannot, for example, dynamically prevent packets originating from or destined for newly discovered malicious network addresses from passing through a PSG at the boundary of a protected network. *See, e.g.*, '213 Patent at 14:56–59. Indeed, every reference in ACNS to changing policy settings involves a manual process for making static changes to an already existing policy rather than receving "a ***non-static*** set of one or more rules, messages, instructions, files, or data structures associated with one or more packets," as the term is properly construed. *See* § III.B, *supra*. While ACNS discloses manually updating settings on the Content Engines, ACNS provides no teaching of a ***dynamic*** security policy located on or received by those Content Engines.

For at least the foregoing reasons, Petitioner has not met its burden to demonstrate that ACNS' Content Engines receive **any** polices, let alone dynamic

security polices, from the Content Distribution Manager. Independent claims 1 and 10, and claims 2-9 and 11-16 are therefore patentable over ACNS at least because ACNS does not disclose "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."

2. ACNS and Kjendal Do Not Teach the Claimed Packet Digest Logging Function (Element [1.2])

Petitioner relies on the teachings of ACNS and Kjendal as allegedly teaching the elements of the claimed packet digest logging recited in independent claims 1 and 10 of the '213 Patent. ACNS and Kjendal fail to disclose this feature of the challenged claims, and Petitioner identifies insufficient motivation to modify ACNS with Kjendal.

(a) ACNS Fails to Disclose Logging Packets on a Packet-By-Packet-Basis

ACNS does not log packets on a packet-by-packet basis. Petitioner alleges that the transaction logging functionality of ACNS maps to the "packet digest logging function" of '213 Patent claims. *See* Petition at 32. Specifically, Petitioner points to Ex. 1008 at 697-707 (19-1 – 19-11) ("Using the Transaction Logs.").

Transaction logs are not logs of individual packets identified as having application-layer packet-header information. *See* '213 Patent, claim 1

("performing…on a packet-by-packet basis…"). To the contrary, ACNS teaches creating a record of each **transaction** requested of the Content Engine. *See* Ex. 1008 at 706-711 (19-10 – 19-15) (describing how to set up a transaction log). As Dr. Goodrich explains, a POSA would understand the transaction logging functionality of ACNS to log transactions between the Content Engine and its clients that meet criteria set up by a user using the GUI shown on 19-10 – 19-11, opposed to logging information about ***each packet*** that includes application-layer packet-header information. *See* Goodrich Decl., ¶¶ 116-124; Ex. 2020 (June 5, 2019 Jeffay Tr.) at 33:1-11 (describing chapter 19 of ACNS as "logging . . .aspects of [a] transaction").

For example, the below example of a transaction logged by ACNS shows that a client made a request ("GET") to the Content Engine to retrieve information from the web address http://www.cisco.com/swa/i/site_tour_link.gif. As explained by Dr. Goodrich, this transaction is 3436 bytes long and would be spread over several packets. Goodrich Decl., ¶¶ 133-134. Notably, the below log entry includes information about the entire transaction—in this case an HTTP GET Request—not about a single packet. *Id.*

> [11/Jan/2003:02:12:44 -0800] "***GET*** ***http://www.cisco.com/swa/i/site_tour_link.gif*** HTTP/1.1" 200 ***3436*** "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"

Ex. 1008 at 699 (19-3).

Indeed, Petitioner admits that ACNS does not log information about packets containing the alleged identified application-layer packet header information on a packet-by-packet basis. Petition at 30. Petitioner's theory further falls apart because it requires logging on a packet-by-packet basis information about the HTTP Request Methods disclosed on ACNS at 8-23 – 8-24. *See* Petition at 28-29 (alleging that ACNS identifies the HTTP request methods of a packets). As shown below, rather than logging packets that include specified application-layer packet-header information, ACNS specifically states that it either logs **every** HTTP request or only those HTTP requests for which user **authentication** had failed:

About Specifying the Transaction Log Entry Type when Logging to a Remote Syslog Host

You can configure the Content Engine to send only the transactions associated with HTTP request authentication failures, or to send all of the transactions.

Typically, organizations are interested in only HTTP request authentication failures for security purposes. By monitoring these types of authentication failures in real time, it enables organizations to identify which end users failed to be authenticated through the Content Engine.

Ex. 1008 at 717 (19-21). Accordingly, ACNS does not teach or suggest that the alleged "packet digest logging function" is to be performed on packets having the specified "application-layer packet-header information" or that it is part of what Petitioner contends is the dynamic security policy received from the CDM.

Indeed, Petitioner acknowledges that "ACNS does not explicitly disclose that the logging function can be applied to log packets based on application-layer packet-header information identified by the HTTP request method or ICAP rules."

Petition at 35. Petitioner instead relies on "Kjendal teach[ing] that packets may be mirrored (i.e. sent to a network logger) based on dynamic rules specifying application-layer packet header information, such as identification of specific application types." *Id.* However, mirroring a packet is **not** a packet digest logging function, regardless of where the mirrored packet is sent. Goodrich Decl., ¶ 121. Indeed, Kjendal's rules do not control what occurs at the network logger, let alone specify that the network logger carry out a specified packet digest logging function. Ex. 1009 at 10:46–49.

That is, simply sending a copy of a packet to a device called a "network logger" is not a packet digest logging function, as claimed, which requires *inter alia* "identifying a subset of information," "generating… a record comprising the subset of information," and "reformatting… the subset of information." *See* '213 Patent, claims 1 and 10. Accordingly, even taken in combination, ACNS and Kjendal fail to disclose receiving a dynamic security policy that includes a rule specifying (1) application-layer packet-header information and (2) a packet digest logging function to be performed upon matching application-layer packet-header information.

For at least these reasons, ACNS in view of Kjendal does not teach or suggest "receiving… a dynamic security policy that comprises at least one rule specifying… a packet transformation function comprising a packet digest logging

function to be performed on packets comprising the application-layer packet-header information," as required by claims 1 and 10.

(b) Petitioner Identified Insufficient Motivation to Combine ACNS with Kjendal

Petitioner asserts that a POSA would have been motivated to combine ACNS with Kjendal "in order to only log packets that are of particular interest and thus avoid logging every packet that comes through the ACNS Content Engines, which could provide unnecessary data that may overwhelm the system." Petition at 31. This argument fails.

Petitioner's argument that Kjendal's selective logging of packets "addressed a specific problem noted in ACNS with respect to the logging of HTTP authentication failures" is inaccurate and supplies no motivation for a POSA to modify ACNS with Kjendal. Goodrich Decl., ¶ 86 (quoting Petition at 36). ACNS utilizes transaction logging to monitor "transaction logs in real-time for particular errors such as authentication errors." Ex. 1008 at 715 (19-19). A POSA would recognize that ACNS authenticates clients that are attempting to utilize the Content Engine. Goodrich Decl., ¶ 88. For example, ACNS might authenticate a client to check whether the client is allowed to access the web. Ex. 1008 at 45 (1-9) ("User Authentication and Content Filtering").

Thus, ACNS's disclosure of logging transactions when a user authentication had failed is not "based on application-layer packet-header information" allegedly

disclosed in Kjendal. Goodrich Decl., ¶ 86 (quoting Petition at 36). Indeed, because information regarding whether a user authentication had failed would be generated at the Content Engine when a user provides incorrect credentials and not an application-layer packet-header, Kjendal's alleged disclosures of selectively mirroring packets based on application-layer packet-header information does **not** address any "specific problem noted in ACNS." Goodrich Decl., ¶ 86 (quoting Petition at 36). Moreover, as acknowledged in the Petition ACNS already discloses a perfectly capable technique for "selectively send[ing] *only* logs of HTTP authentication failures to the syslog server." Petition at 36.

Petitioner's argument that "[a] POSA would understand that an administrator of the ACNS system could also choose to selectively log other types of application-layer information" also fails to provide sufficient motivation to combine ACNS and Kjendal for several reasons. Goodrich Decl., ¶ 86 (quoting Petition at 36).

First, although Petitioner argues that the ACNS administrator **could** "choose to selectively log other types of application-layer information," Petitioner does not explain why such an administrator **would** do so, which is insufficient as a matter of law. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) ("[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art

to arrive at the claimed invention.") (emphasis original) (citation omitted). *Second*, the question is not whether an administrator would have "cho[sen] to selectively log other types of application-layer information," but whether a POSA would have modified ACNS, which by Petitioner's admission "does not explicitly disclose that the logging function can be applied to log packets **based on** the application-layer packet-header information," with Kjendal. Petition at 35-36 (emphasis added).

Third, whether or not there are "benefits of filtering packets before mirroring to another device (i.e. for logging) in order to reduce the chances of overloading the target of the mirrored packets" within the context of Kjendal, Petitioner identifies no reason that the same technique would be beneficial in the context of ACNS. *Id.* at 36-37. In fact, because ACNS does not operate on packets at all (as it operates instead on requests) there is no "chance[] of overloading the target of the mirrored packets." Furthermore, ACNS's transaction logs are not created on any other "target"—whether the target be of mirrored packets or mirrored requests—so there simply is no chance of overloading such a target.

(c) There is no Reason to Modify ACNS with Kjendal

A POSA would not be motivated to combine ACNS and Kjendal because they teach fundamentally different logging techniques. Goodrich Decl., ¶¶ 86-94. ACNS teaches transaction logging, not packet logging. Ex. 1008 at 697-715 (19-1 – 19-22). In transaction logging, a system would log information about an entire

transaction (e.g., a failure to authenticate a transaction, a time stamp of the transaction, etc.) between two devices, such as the Content Engine and a client, rather than logging information about an individual packet. *Id.* at 715 (19-19). Each transaction in ACNS is typically spread over multiple packets because transaction are often larger than the maximum transmission unit (MTU) limits the size of a single network-layer packet or, depending on the link-layer protocol, the maximum size of a link-layer packet. Goodrich Decl., ¶ 87. This type of transaction logging does not log information about each packet contained in the transaction, but instead logs information about the transaction as a whole, such as information about an HTTP Request or Response. *Id.*

On the other hand, Kjendal teaches a technique for mirroring network traffic based on multiple criteria. Ex. 1009, Abstract. Specifically, Kjendal can begin and end the mirroring of traffic based on the following criteria:

> [C]riteria which may generate a mirroring activity include, but are not limited to, frames of packets, the content of particular fields in a frame, flow counts, the end of a flow, a regularly timed mirroring initiation or any other conditions of interest to the network administrator can be used as conditions for establishing mirroring activities on a device of the network. In addition, events or criteria may be established for stopping the mirroring function. For example, a mirroring activity may be stopped based on the data value in a packet field, a network, regional or device specific event, a simple count of packets or other flow metric,

> a time out, the end of flow or based on a change in a prioritization condition (i.e., a condition has occurred wherein mirroring must be performed on a different flow that has been designated as being of higher priority for mirroring, particularly when the device carrying out the mirroring has limited capacity in that regard.

Id. at 10:1-17.

As shown above, Kjendal mirrors packets based identifying a criteria associated with the flow of traffic (e.g., recognizing the presence of a particular field in a flow of packets). A POSA would recognize that ACNS and Kjendal teach fundamentally different approaches because Kjendal is not concerned with the information spanning over the multiple packets in a transaction, such as whether a transaction is authenticated. Goodrich Decl., ¶ 90. Instead, Kjendal is concerned with mirroring packet flows based off various criteria that would not identify, or be specific to, a transaction. Combining these two approaching into a workable combination would require undue experimentation and would not result in predictable results. *Id*.

Additionally, Petitioner asserts that "a POSA would have been motivated to implement these teachings of Kjendal into ACNS in order to only log packets that are of particular interest and thus avoid logging every packet that comes through the ACNS Content Engines, which could provide unnecessary data that may overwhelm the system." Petition at 31. However, Petitioner is creating a problem

that simply does not exist within ACNS. ACNS teaches logging either all transactions or all HTTP request authorization failures, as shown below. ACNS does not incur the problem of "logging every packet that comes through the ACNS Content Engine," as Petitioner asserts, because it logs transactions.

Further, absent using the '213 Patent as a guide or blueprint, there is no identified deficiency in ACNS that would motivate a POSA to look to Kjendal to fill a technological void. Goodrich Decl., ¶ 93. For example, ACNS states of its solution, "[t]ypically, organizations are interested in ***only*** HTTP request authentication failures ***for security purposes***." Ex. 1008 at 717 (19-21) (emphasis added). Indeed, ACNS does not even mention a need to log information about individual packets to satisfy its security concerns. While Dr. Jeffay states that A POSA would be motivated to incorporate the traffic flow mirroring of Kjendal into the transaction logging functionality of Kjendal because there's a probability that a "packet has some indictor that it is a security threat or is objectionable" (Jeffay Decl., ¶ 166), ACNS does not recognize any such deficiency or concern with packet security.

Further, incorporating the teachings of Kjendal into ACNS would change the operating principle of ACNS. ACNS teaches transaction logging functionality to log all Content Engine transactions or all HTTP request authorization failures. Ex. 1008 at 717 (19-21). The packet mirroring technology of Kjendal, if added to

ACNS' transaction logging, would change the logging operations of ACNS. In fact, Dr. Jeffay fails to explain how ACNS would perform both transaction logging and packet logging simultaneously. Jeffay Decl., ¶¶ 148, 166. Further, modifying ACNS to log network packet traffic using the criteria taught by Kjendal would change the operating principle of ACNS because logging network traffic would not assist in ACNS' primary function of caching content and recording transaction requests and responses from web clients for content. *See* Goodrich Decl., ¶ 94.

Hence, for at least these reasons, there is no motivation to combine ACNS with Kjendal.

3. Petitioner Has Not Demonstrated that ACNS in View of Kjendal Discloses Identifying Packets With Application-Layer Packet-Header Information on a Packet by Packet Basis (Element [1.4])

Contrary to Petitioner's contention, ACNS and Kjendal, taken alone or in combination, fail to teach or suggest "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information." As a preliminary note, Petitioner does not assert that Kjendal teaches or suggests identifying packets with application-layer packet-header information on a packet-by-packet basis. *See* Petition at 39-40.

(a) ACNS Does Not Identify Packets on a Packet-By-Packet Basis

In the context of the '213 Patent, the term "packet" refers to an L2 or L3 layer packet based on the OSI Model. *See* § III.A, *supra*. Petitioner's argument as to how ACNS allegedly teaches this claim element relies on a fundamental misinterpretation of the subject matter recited in the '213 Patent. Rather than identifying packets that include the recited "application-layer packet-header information" on a **packet-by-packet** basis, ACNS must reassemble the payloads of the packets of HTTP (web) communications flows before determining whether or not a web object should be cached or whether a request for web content should be logged. Goodrich Decl., ¶ 118. In other words, the techniques disclosed in ACNS do **not** include packet-filtering rules that are used to identify packets that include specified application-layer packet-header information on a "packet-by-packet basis." *Id.*

The ability to identify packets including specified application-layer packet-header information on a packet-by-packet basis is described throughout the '213 Patent. In fact, Petitioner's expert admits that "[a] POSA would understand that a rule requiring [identifying] packet-header information…must first identify, on a packet-by-packet basis, each packet comprising [] application-layer packet-header information." Jeffay Decl., ¶ 173; *see also* Ex. 2009 (April 18, 2019 Jeffay Tr.) at 48:8–16 (admitting that the term "packet-by-packet" means that "you're working a

packet at a time"). In other words, the L2/L3 "packets comprising the application-layer packet-header information" are identified because they match the condition specified by the "rule specifying application-layer packet-header information" recited earlier in the claim. *See* '213 Patent, claim 1. In view of the foregoing, the '213 Patent is generally directed to (1) receiving L2/L3 packets, (2) identifying, on a packet-by-packet basis, those L2/L3packets that include application-layer packet-header information specified by a rule of a dynamic security policy, and (3) performing a packet transformation function on each identified packet, again on a packet-by-packet basis. Goodrich Decl., ¶ 126. ACNS does **not** identify packets comprising specified application-layer packet-header information on a "packet-by-packet" basis.

Petitioner first cites to Chapter 8 of ACNS as allegedly teaching "examin[ing] the application-layer packet-header of HTTP packets to determine whether the HTTP request method is supported by the Content Engine." Petition at 39-40; Jeffay Decl., ¶ 173 (citing EX1008, p. 8-23). However, ACNS must reassemble L2 and/or L3 packets received by the Content Engine to identify the request method. As Dr. Goodrich explains, a POSA would understand that HTTP request methods such as POST are often spread over several L2 and/or L3 packets. Goodrich Decl., ¶ 128. As shown below, ACNS looks at the entire HTTP request

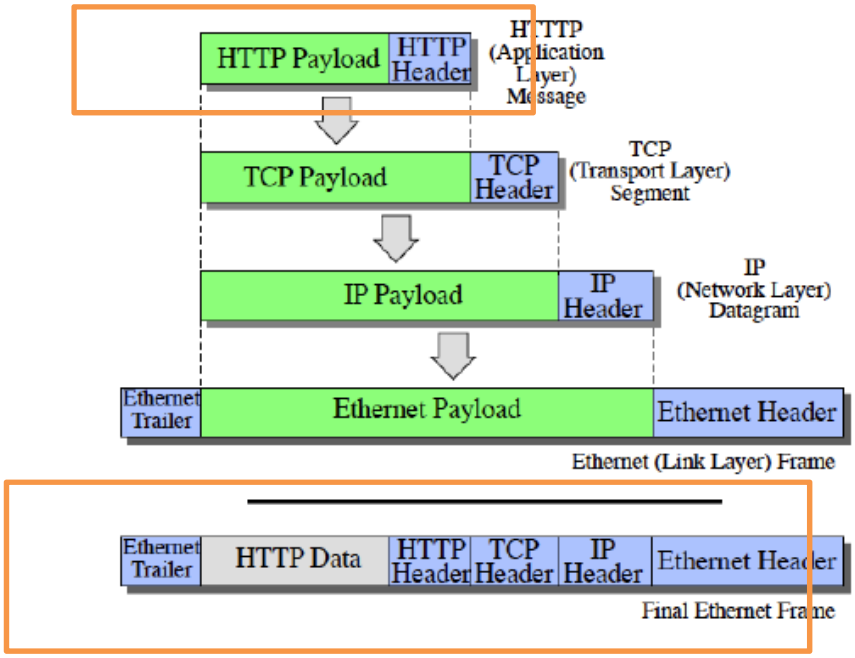
that is received from a client, which may be transmitted over multiple packets, to determine whether the HTTP request method is supported.

> Content Engines accept or reject an HTTP request depending on whether the HTTP request method is supported. HTTP 1.1 request methods (for example, GET, HEAD, or POST) are supported by default. Nonstandard request methods, such as Web-Based Distributed Authoring and Versioning (WebDAV) are not.
>
> ***When the Content Engine receives an HTTP request from a client using an unsupported method***, ACNS software adds the method to the list of unsupported methods and sends an error to the client. You can use the Creating New HTTP Method for Content Engine window to add a method to the list of methods already supported by the Content Engine.

Ex. 1008 at 341 (8-23).

Furthermore, ACNS cannot identify application-layer packet header information in an HTTP request without reassembling the packets that make up the request because ACNS cannot inspect the payload of an L2 or L3 packet. *See* II.A *supra*. Dr. Jeffay testified that ACNS is not capable of inspecting the payload of packets. Ex. 2020 (June 5, 2019 Jeffay Tr.) at 68:16-69:16 (Q: "why do you say ACNS doesn't allow you to . . . directly inspect the payloads to see if there's malware in the payload?" A: "Because I don't believe ACNS discloses the ability to do searching, for example, over payloads."). As shown below (identified in

orange boxes), the HTTP header information is located inside the payload of both L2 (link layer) and L3 (Network Layer) packets:



Jeffay Decl., ¶ 51. Accordingly, by Dr. Jeffay's own admission, ACNS is not capable of inspecting L2 and L3 packets that ACNS receives for application-layer packet-header information. *See* Ex. 2020 (June 5, 2019 Jeffay Tr.) at 68:16-69:16.

Petitioner also states that ACNS teaches that the Content Engine identifies "packet-header information" using Internet Content Adaption Protocol ("ICAP") server functionality. Petition at 40. However, identifying "packet-header information" does not satisfy this claim limitation. Petitioner points to ICAP "rule actions" at ACNS pages 16-15 – 16-25 as "identifying packets using, for example, an application-layer packet-header information such as URL and Request Method." *Id.* However, Dr. Jeffay again acknowledged that these ICAP server

rule actions are applied to content requests or content responses, not individual packets. *See* Ex. 2020 (June 5, 2019 Jeffay Tr.) 58:4-11 (stating that the rule actions listed in Table 16-6 are applied to web requests and responses). Indeed, as Dr. Goodrich opines, the Content Engines in ACNS are concerned with content management, which deals specifically with receiving content requests and content responses. Goodrich Decl., ¶ 67. The Content Engines are not concerned with applying rules to individual packets. *Id.*; *see also* Ex. 1008 at 38 (1-2) ("[t]he primary role of a Content Engine in the ACNS network is to serve client requests for content.").

For at least the foregoing reasons, ACNS and Kjendal, taken alone or in combination, fail to disclose "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."

4. ACNS Fails to Teach Identifying a Subset of Information Specified By the Packet Digest Logging Function (Element [1.6])

Contrary to Petitioner's contention, ACNS fails to teach or suggest "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information," as recited by claim 1.

Petitioner asserts that ACNS' disclosure of "transaction logs" teaches identifying (and logging) a subset of information for each of the packets identified as having application-layer packet-header information. Petition at 42-43. Petitioner relies on the following example of a transaction log on page 19-1 of ACNS:

> 1012429341.115 100 **172.16.100.152** TCP_REFRESH_MISS/304 1100 **GET http://www.cisco.com/images/homepage/news.gif** - DIRECT/www.cisco.com –

Petition at 42; Ex. 1008 at 697 (19-1).

Petitioner further highlights various entries (indicated above in bold) in the above transaction log to allege that ACNS teaches identifying a subset of information in each packet identified as having application-layer-packet header information. Petition at 42. However, the above log entry shows logging a subset of information about a transaction, not a packet. Goodrich Decl., ¶¶ 131-136. Indeed, as Dr. Goodrich explains, transaction logging works by identifying and recording a subset of information in a transaction reconstructed from the payloads of multiple individual packets. *Id.* In another example, ACNS discloses the structure of the ACNS transaction logging as follows:

> **transaction-logs format custom "[%{%d}t/%{%b}t/%{%Y}t:%{%H}t:%{%M}t:%{%S}t %{%z}t] %r %s %b %{Referer}i %{User-Agent}i"**
>
> The following transaction log entry example in the Apache Combined Format is configured by using the preceding custom format string:

> [11/Jan/2003:02:12:44 -0800] "GET http://www.cisco.com/swa/i/site_tour_link.gif HTTP/1.1" 200 **3436** "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"

Ex. 1008 at 699 (19-3).

The transaction log example above shows, for example, that the transaction was 3436 bytes of information, which would have been divided over several packets because the maximum transmission unit (MTU) size of an L2/L3 packet is 1,500 bytes. Goodrich, Decl., ¶ 134. This example shows that (1) the transaction occurred over several packets, and not a packet-by-packet basis as claim 1 recites, and (2) logging the byte size of the transactions shows that a subset of information about the transaction was logged, not a subset of information about each packet identified as having application-layer packet-header information. *Id.* ACNS' disclosure of transaction logging demonstrates that ACNS logs information at the transaction level and not of individual packets and that a transaction is often spread over multiple L2/L3 packets. Accordingly, ACNS does not teach or suggest identifying a subset of information for ***each packet*** identified as having application-layer packet-header information.

Additionally, the explicit language of the claims does not merely require logging "any subset of information," as characterized in the Petition. Petition at 42. Rather, the claim language recited in element 1.6 requires "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." Petitioner does not assert that ACNS discloses a packet digest logging function that specifies the subset of information to be logged for each packet meeting a rule's criteria, or that such a modification to Kjendal would have been obvious, as is its obligation under 37 C.F.R. § 42.104(b)(4).

Implementing a packet digest logging function as a packet transformation function permits the "information specified by the packet digest logging function" to be tailored to the condition matched by the rule, which among other benefits, enhances the ability of the '213 Patent's "[a]wareness application servers… to produce awareness information." Goodrich Decl., ¶ 135 (citing '213 Patent at 11:34–60). Because ACNS does not disclose a rule comprising a packet digest logging function that specifies the "subset of information," ACNS lacks the ability to log packet information with the level of granularity and specificity enabled by the techniques claimed in the '213 Patent. *Id*.

Accordingly, ACNS fails to teach or suggest "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information," as recited by claim 1.

5. ACNS Fails to Teach Generating a Record for Each Packet Identified as Having Application-Layer Packet-Header Information (Element [1.7])

As a preliminary matter, ACNS fails to disclose the claimed "packet digest logging function" and cannot therefore disclose element 1.7, which recites "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." *See* § V.A.2.a, *supra*.

Petitioner argues that ACNS disclosure of transaction logging teaches this limitation and that "[a] POSA would understand that ACNS software generates a record of the information…for use in writing a log entry in one of the specified or custom formats." Petition at 43. This limitation is directed at generating a record "**for each of the one or more packets** comprising application-layer packet header information." The transaction logging of ACNS does not perform logging at the granular level of logging information about each packet, as discussed above. *See* § V.A.4, *supra*; Goodrich Decl., ¶ 138. Petitioner cites no evidence for the bald assertion that ACNS generates a record for **each packet** identified in Element [1.4] other than the declaration of its expert, Dr. Jeffay, who merely parrots the same conclusory assertion without any underlying evidence. *See* Jeffay Decl., ¶ 183. Accordingly, Dr. Jeffay's opinion should be accorded little or no weight. *See Kinetic Techs., Inc. v. Skyworks Solutions, Inc.*, Case IPR2014-00529, Paper 8 at

14–15 (P.T.A.B. Sept. 23, 2014) ("Merely repeating an argument from the Petition in the declaration of a proposed expert does not give that argument enhanced probative value."); *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

6. ACNS and Kjendal Do Not Teach Routing the Identified Packets to a Monitoring Device in Response to Performing the Packet Transformation Function (Element [1.9])

Petitioner has not demonstrated that Kjendal discloses "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function." As a preliminary matter, Petitioner does not assert that ACNS meets this claim limitation. *See* Petition at 45-47.

Kjendal fails to disclose this element of the challenged claims at least because it does not disclose routing "packets corresponding to the application-layer packet-header information ***in response to*** the performing the packet transformation function" on a packet-by packet basis. Indeed, Petitioner fails to even allege that either ACNS or Kjendal teach that routing is performed in response to performing a packet transformation function. *Id.*

Kjendal's techniques are directed to mirroring packet flows based on criteria rather than routing packets on a packet-by-packet basis to a monitoring device ***in response*** to performing a packet transformation function on those packets. Goodrich Decl., ¶¶ 140-143. For example, Kjendal teaches the following traffic flow mirroring techniques:

> The dynamic traffic mirroring function can do at least one or more of: 1) mirror all or any portion of the flow, such as the first N packets, the first M fields, the first L Bytes, selected fields and one-way or bidirectional flows; 2) define flows by source address-destination address, Tuple, 5-tuple, application, etc.; and 3) transport the packets by portals to generalized or specific destinations.

Ex. 1009 at 8:64–9:3.

However, claim 1 requires that these packets be routed in response to a packet transformation function being applied to the packets. The Institution Decision has construed the term "packet transformation function" to mean "operations performed on a packet." *See* Institution Decision at 13. Thus, to meet this claim limitation, Petitioner must show that Kjendal routes packets in response to an operation being performed on the packets. However, that is not how Kjendal functions. As discussed above, Kjendal mirrors packet flows based on identifying certain criteria in the packet flow. Indeed, particularly in the case of claim 1 of the

'213 Patent, where the claim recites that a packet transformation function comprises:

> **(1)** 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;
>
> **(2)** 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
>
> **(3)** 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

'213 Patent at 25:38-50.

Indeed, Kjendal's disclosure of mirroring packets that have been identified as meeting a criteria, e.g. having the presence of a selected field, does not teach "routing…on a packet-by-packet basis, to a monitoring device each of the one or more packets…***in response to the performing the packet transformation function***," as recited by claim 1.

B. ACNS in View of Kjendal and DiffServ Does Not Render Obvious Claims 10–16

The combination of ACNS in view of Kjendal, and DiffServ does not render challenged claims 10–16 obvious under 35 U.S.C. § 103.

1. Petitioner Has Not Demonstrated that ACNS in View of Kjendal, and DiffServ Discloses Receiving a Dynamic Security Policy From a Security Policy Management Server (Elements [10.1] & [10.2])

As discussed above, Petitioner has not met its burden to demonstrate that ACNS in view of Kjendal discloses "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." *See* § V.A.1, *supra*. Petitioner relies on the same deficient arguments for its application of ACNS and Kjendal to independent claim 10. *See* Petition at 62-64.

Petitioner's argument with respect to claim 10 fails for the same reasons that it fails for claim 1—namely, that neither ACNS nor Kjendal discloses receiving a dynamic security policy from a security policy management server. *See* § V.A.1, *supra*. Accordingly, Patent Owner requests that the Board find claim 10 and claims 11–16, which depend therefrom, patentable over ACNS in View of Kjendal, and DiffServ.

2. Petitioner Has Not Demonstrated that ACNS in View of Kjendal, and DiffServ Discloses Receiving a Dynamic Security Policy With a Rule That Includes a DSCP Selector as the Packet Identification Criteria (claims 10–16)

Petitioner has not met its burden to demonstrate that the cited references disclose "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 packet-identification criteria…, wherein the packet-identification criteria comprises a Differentiated Service Code Point (DSCP) selector." '213 Patent, claim 10.

Petitioner argues that "[t]he combination of ACNS and DiffServ teaches" "wherein the packet-identification criteria comprises a Differentiated Service Code Point (DSCP) selector." Petition at 64. It does not. To the extent that ACNS and DiffServ disclose utilizing DSCP data, it is used for packet classification prior to the application of any security policy and not as the packet-identification criteria specified by a dynamic security policy. Goodrich Decl., ¶¶ 151-153.

Petitioner argues that DiffServ discloses "'classifier' rules" that qualify as "packet identification criteria for the purposes of claim 10 and its dependent claims." Petition at 63. However, the combination is unsupported and does not reach the claimed subject matter because the "rule" that DiffServ's "[p]acket classifiers" would still not be packet-identification criteria in a received dynamic security policy. Goodrich Decl., ¶¶ 151-153.

For at least the foregoing reasons, the cited references fail to disclose, alone or in combination, "receiving… a dynamic security policy that comprises at least one rule specifying packet-identification criteria, … corresponding to the packet-identification criteria, wherein the packet-identification criteria comprises a

Differentiated Service Code Point (DSCP) selector," as recited in independent claim 10.

3. Petitioner Has Not Demonstrated that ACNS in View of Kjendal and Diffserv Discloses Identifying Packets With the Packet-Identification Criteria on a Packet by Packet Basis (claims 10–16)

As discussed above, Petitioner has not met its burden to demonstrate that ACNS in view of Kjendal discloses "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." *See* § V.A.3, *supra*. Petitioner relies on the same deficient arguments for its application of ACNS and Kjendal to independent claim 10. *See* Petition at 62-64.

Petitioner's argument with respect to claim 10 fails for the same reasons that it fails for claim 1—namely, that ACNS and Kjendal do not disclose a dynamic security policy rule that identifies packets based on packet-identification criteria on a packet-by-packet basis. *See* § V.A.3, *supra*. Accordingly, Patent Owner requests that the Board find claim 10 and claims 11–16, which depend therefrom, patentable over ACNS and Kjendal.

4. Petitioner Has Not Demonstrated that ACNS in View of Kjendal, and DiffServ Discloses "routing… to a monitoring device" (claims 10–16)

As discussed above, Petitioner has not met its burden to demonstrate that ACNS and Kjendal disclose "routing … to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function," as recited in independent claim 1." *See supra* § V.A.6. Petitioner relies on the same deficient arguments for its application of Kjendal to independent claim 10. *See* Petition at 68-69.

Petitioner's argument with respect to claim 10 fails for the same reasons that it fails for claim 1, and for at least the foregoing reasons, the combination of ACNS, Kjendal, and DiffServ fails to disclose "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 packet-identification criteria in response to the performing the packet digest logging function" as recited in independent claim 10. Patent Owner respectfully requests, therefore, that the Board find patentable claim 10 and claims 11–16, which depend therefrom.

VI. OBJECTIVE INDICIA OF NONOBVIOUSNESS

As the United States Supreme Court and the Federal Circuit have repeatedly stated, any obviousness analysis must include (1) the scope and content of the prior

art, (2) the differences between the prior art and the claims at issue, (3) the level of ordinary skill in the pertinent art, and (4) relevant secondary considerations of non-obviousness. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Failure to address any one of these criteria is fatal to a challenger's obviousness argument as a matter of law. *See, e.g., Apple Inc. v. Int'l Trade Comm'n*, 725 F.3d 1356, 1365–66 (Fed. Cir. 2013) (vacated and remanded ITC's ruling of obvious, as ITC failed to consider all obviousness factors, including objective evidence of secondary considerations); *Ruiz v. A.B. Chance Co.*, 234 F.3d 654, 660, 667-68 (Fed. Cir. 2000) (vacated a conclusion of obviousness because the fact-finder failed to make *Graham* factor findings).

"Objective indicia 'can be the most probative evidence of nonobviousness in the record, and enables the court to avert the trap of hindsight.'" *Leo Pharm. Prods., Ltd. v. Rea*, 726 F.3d 1346, 1358 (Fed. Cir. 2013) (quoting *Crocs, Inc. v. Int'l Trade Comm'n*, 598 F.3d 1294, 1310 (Fed. Cir. 2010)) ("Here, the objective indicia of nonobviousness are crucial in avoiding the trap of hindsight when reviewing, what otherwise seems like, a combination of known elements."). In other words, objective indicia of nonobviousness must always be considered. *Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1354-55 (Fed. Cir. 2013). Such evidence "cannot be overlooked" and indeed can "serve to resist the temptation to read into the prior art teachings of the invention in issue." *Id.* (quoting *In re*

Cyclobenzaprine Hydrochloride Extended–Release Capsule Patent Litig., 676 F.3d 1063, 1076 (Fed. Cir. 2012)); *see also Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013) (overturning Board because it failed to properly consider objective indicia of nonobviousness).

Centripetal's patented inventions have received significant praise and commercial success. This evidence on its own is enough to overcome Petitioner's challenges to the obviousness of the '213 Patent. *See Institut Pasteur & Universite Pierre Et Marie Curie v. Focarino*, 738 F.3d 1337, 1346-47 (Fed. Cir. 2013) (evidence that competitors "praised, and copied" claimed inventions served as dispositive objective indicia of non-obviousness).

A. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others

The failure of others can result in a strong indication of non-obviousness. *See In re: Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d at 1075 (reversing district court and finding evidence of unexpected results and long-felt need for those results supported a finding of non-obviousness). Failure of others is also indicative of unexpected results and long-felt need because one of ordinary skill in the art would not reasonably expect the success. *See id; see also Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1382 (Fed. Cir. 1983) (holding that the lack of previous attempts to achieve the results of the invention indicated a lack of long-felt need).

The '213 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to provide proactive network protection that could "scale to larger networks." Goodrich Decl., ¶ 159 (citing '213 Patent at 1:20–21). In 2010, the US Naval Research Laboratory hosted "Computer Network Defense/Information Assurance (CND/IA) Enabling Capability (EC) Industry Day" where Stanley Chincheck, the Director for Center for High Assurance Computer Systems, explained that previous strategies for protecting networks could not keep up with changes in the environment. Ex. 2013 (Computer Network Defense/Information Assurance Enabling Capability) at 5. In particular, he demonstrated via the chart reproduced below that "Signature-based defense of host A/V and network firewalls are ineffective… We need new ways to frame, understand and reverse these trends." *Id.* at 6; Goodrich Decl., ¶ 160.

Ex. 2013 (Computer Network Defense/Information Assurance Enabling Capability) at 6. The failure of signature behavior based systems, such as the ones disclosed in ACNS, to keep up with emerging threats demanded new solutions. Goodrich Decl., ¶ 160. Accordingly, the long felt need for the solution provided by the '213 Patent was recognized at least as far back as 2010. *Id*.

The failure of others in the industry to provide proactive network protection that could scale to larger networks and meet emerging threats was recognized in the White Paper entitled "Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-Led

Enforcement." Ex. 2006 at 1 ("ESG Paper"). In particular, the ESG Paper recognized that "[t]he promise of cyber threat intelligence (CTI) for cyber-defense has been talked about for years" and that the manual processes most enterprises have in place for using CTI "don't scale well and the forensic focus on security emergencies can cause enterprises to miss out on the benefits of proactive, preventive intelligence-based defense." *Id.* at 3. This inability for traditional systems to provide proactive, scalable network-protection services was the same problem identified in the BACKGROUND section of the '213 Patent. '213 Patent at 1:15–27; Goodrich Decl., ¶ 161.

The ESG Paper further acknowledged that "[t]he end goal of a threat intelligence program is defense in advance of an event" and identified "multiple challenges stand in the way of operationalizing threat intelligence in a high performance, and high-fidelity way," including "[l]ack of automation," the inability to use feeds "in a meaningful way to live network traffic and even less frequently applied inline for a protective benefit," and the ability to "turn[] CTI into actionable insight." Ex. 2006 at 4. Into this morass stepped Centripetal Networks:

> Centripetal Networks' CleanINTERNET intelligence-led managed security service using their RuleGATE enforcement point provides customized threat intelligence filtering designed to significantly reduce security event volume and workload in the enterprise. Centripetal

> shields the network and dynamically monitors for advanced threats using intelligence. **Centripetal's goal is nothing less than the transformation of CTI into protective action at scale. Centripetal does this by converting indicators to rules that drive actions** across a risk spectrum, i.e., **logging, content capture, mirroring, redirection**, shielding, and advanced threat detection.

Id. at 7 (emphasis added); Goodrich Decl., ¶ 162.

This laudatory description of Centripetal's solution to the long felt need of how to meaningfully operationalize CTI is tied to the invention disclosed and claimed in the '213 Patent. Goodrich Decl., ¶ 163. The claims of the '213 Patent are generally directed to receiving a "dynamic security policy" from a "security policy management server." *See* '213 Patent, claims 1 and 10. The "dynamic security policy" is distinguished from prior art security policies in that it is managed on a central server (the claimed SPM) and is "dynamic" in that it is automatically updated when new CTI (*i.e.* "new network addresses associated with malicious network traffic") is received at the SPM (*e.g.* from a "malicious host tracker service"). *See* §§ III.B, V.A.1, *supra*; '213 Patent at 3:15–21; 14:48-15:37; Goodrich Decl., ¶ 163.

This technique contributes to Centripetal's ability to "better manage traffic by leveraging CTI context with highly granular rules in the form of policies that can be automatically enforced." Ex. 2006 at 7; Goodrich Decl., ¶ 164. In fact, the

ESG Paper describes that during its test of an embodiment of the PSG recited in the claims of the '213 Patent (*i.e.* Centripetal's Threat intelligence Gateway, RuleGATE), "[t]he intelligence was dynamically updated without loss and the results were reported in real time for live analytics." Ex. 2006 at 7. Furthermore, the packet transformation functions explicitly claimed in the '213 Patent, including the packet digest logging function and routing packets meeting the specified criteria were specifically cited in the ESG Paper as helping to achieve the of "transformation of CTI into proactive action at scale." *Id.*; Goodrich Decl., ¶ 164.

The ESG Paper also praises the performance of Centripetal's Threat Intelligence Gateway as "the highest performance network filter that ESG has tested or seen in action to date," contrasting Centripetal's products "with firewalls and IPS systems, which aren't designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds." Ex. 2006 at 7–8. Dr. Goodrich explains that the best-in-class performance of Centripetal's TIG owes in large part to the fact that the dynamic security policies implement rules on a packet-by-packet basis, allowing the TIG to operate as a "network filter" rather than a traditional IPS that performs "deeper inspection of the application layer." Ex. 2006 at 1; Goodrich Decl., ¶ 165.

Given the foregoing evidence of Centripetal's success in solving the long felt need of operationalizing CTI, the '213 Patent is non-obvious.

B. Industry Praise

Products embodying the invention claimed in the'213 Patent have received substantial industry praise. For example, the ESG Paper discussed above praised Centripetal's TIG as having "the highest performance network filter that ESG has tested or seen in action to date." Ex. 2006 at 8. The ESG Paper further lauded Centripetal's TIG ability to "deliver[] more than is possible with firewalls and IPS systems":

> Simply put, Centripetal delivers more than is possible with firewalls and IPS systems, which aren't designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds. ESG watched as Centripetal Networks' Threat Intelligence Gateway solution processed over 140 Gbps of network traffic at wire speed; distributing, ingesting, synthesizing into a network policy, and enforcing over five million complex network filtering rules. Each complex filtering rule contained at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state. With intelligence enforcement there can be no presumption of insider trust so traditional filters' state assumptions are invalid.

Ex. 2006 at 7; Goodrich Decl., ¶ 167.

Furthermore, on May 4, 2017, Gartner published its "Cool Vendors in Security for Technology and Service Providers," praising Centripetal as being "unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds." Ex. 2007 (Gartner –

Cool Ventors) at 5. As described in the Cool Vendors article, Centripetal's QuickThreat Gateway "currently has the largest number of third-party threat intelligence service integrations in the network security market. It claims to be able to use up to 5 million indicators simultaneously." *Id*. Centripetal Network s was also named one of American Banker's "Top 10 FinTech Companies to Watch" for 2014 because its Threat Intelligence Gateway, RuleGATE "has the potential to detect and deter rapidly changing cybersecurity threats on the fly." Ex. 2011 (Top 10 FinTech Companies) at 14; Goodrich Decl., ¶ 168.

As discussed directly above, the salutary benefits of Centripetal's TIG discussed in the ESG Paper and the Cool Vendors article are made possible in large part by the '213 Patent's dynamic security policies, which are automatically managed and distributed by the claimed SPM, as well as its network layer packet-by-packet rule enforcement, packet digest logging function and packet transformation function for routing packets to a monitoring device. *See* § V.A, *supra*; Goodrich Decl., ¶ 169. Accordingly, the industry praise the products embodying the '213 Patent have received in the industry further demonstrates that the '213 Patent was not obvious.

C. Commercial Success and Licensing

"When a patentee can demonstrate commercial success, usually shown by significant sales in a relevant market, and that the successful product is the

invention disclosed and claimed in the patent, it is presumed that the commercial success is due to the patented invention." *GrafTech Int'l Holdings, Inc. v. Laird Techs., Inc.*, 652 F. Appx. 973, 979 (Fed. Cir. 2016) (quoting *J.T. Eaton & Co. v. Atl. Paste & Glue Co.*, 106 F.3d 1563, 1571 (Fed. Cir. 1997)). The commercial success of the patented inventions disclosed in the '213 Patent is evidenced through the declaration of Jonathan Rogers, Centripetal's Chief Operating Officer, who testified to the significant success of the RuleGATE product, which embodies the '213 Patent. Ex. 2016 (Declaration or Jonathan Rogers).

The fact that companies have taken a license to the '213 Patent is powerful evidence of non-obviousness. *See Minnesota Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1575 (Fed. Cir. 1992) (stating that taking a license "provide[s] a colorful picture of the state of the art, what was known by those in the art, and a solid evidentiary foundation on which to rest a nonobviousness determination."). In October 2018, Keysight Technologies took "a worldwide, royalty-bearing, non-transferable, irrevocable, nonterminable, non-exclusive license to Centripetal's worldwide patent portfolio," including the '213 Patent. Ex. 2012 (KeySight Technologies, Inc. Annual Report) at 83. Aside from ongoing royalties, the agreement included a "one-time payment of $25 million for past damages." *Id.*

Because Centripetal's licensees sell products that embody the inventions claimed in the '213 Patent, and those licensees are in the same security market as Petitioner, a presumption exists that the commercial success of Centripetal's licensees products is due to the patented invention of the '213 Patent. Consequently, the fact that licensees entered into a license agreement, which included a license to the '213 Patent, to avoid litigation and to continue conducting business, including selling and offering for sale products that encompass the patented technology licensed from Centripetal shows that there is a nexus between these license agreements and the Challenged Claims of the '213 Patent. Therefore, the commercial success of products that embody the inventions disclosed in the '213 Patent and the successful licensing of the '213 Patent demonstrate that the '213 Patent is not obvious.

VII. CONCLUSION

Petitioner has not established by a preponderance of the evidence that the challenged claims 1–16 of the '213 Patent are invalid. Centripetal accordingly requests that the Board find claims 1–16 patentable.

Respectfully submitted,

Dated: July 5, 2019

/James Hannah/

James Hannah (Reg. No. 56,369)
Michael Lee (Reg. No. 63,941)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road

Menlo Park, CA 94025
Tel: 650.752.1700 Fax: 212.715.8000

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502 Fax: 212.715.8302

Bradley C. Wright (Reg. No. 38,061)
Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200,
Washington, DC 20005.
Tel: 202.824.3160. Fax: 202.824.3000.
Email: bwright@bannerwitcoff.com.

(Case No. IPR2018-01512) *Attorneys for Patent Owner*

PATENT OWNER'S EXHIBIT LIST

Exhibit-2001	Opinion and Order re Claim Construction, *Centripetal Networks, Inc., v. Keysight Tech's, Inc., et al*., No. 2:17-cv-00383 (Dkt. 484).
Exhibit-2002	Amended Joint Claim Construction Statement, Exhibit 2, *Centripetal Networks, Inc., v. Keysight Tech's, Inc., et al*., No. 2:17-cv-00383 (Dkt. 244-2).
Exhibit-2003	Intentionally Omitted
Exhibit-2004	Declaration of Dr. Michael Goodrich in Support of Patent Owner's Response with Appendix A (CV)
Exhibit-2005	Intentionally Omitted
Exhibit-2006	ESG White Paper – Centripetal Networks Threat Intelligence Gateway, by Tony Palmer (May 2018)
Exhibit-2007	Gartner – Cool Vendors in Security for Technology and Service Providers, 2017, published May 4, 2017
Exhibit-2008	Excerpts from Tanenbaum, *Computer Networks*, 5th edition, Prentice-Hall, 2011
Exhibit-2009	Deposition Transcript of Dr. Kevin Jeffay in IPR2018-01386, taken on April 18, 2019
Exhibit-2010	Gupta and McKeown, *Algorithms for Packet Classification*, IEEE NETWORK, March/April 2001.
Exhibit-2011	American Banker article, "Top 10 FinTech Companies to Watch," published November 6, 2013.
Exhibit-2012	KeySight Technologies, Inc. Annual Report 2018
Exhibit-2013	Stanley Chincheck, US Naval Research Laboratory, Computer Network Defense/Information Assurance (CND/IA) Enabling Capability (EC) Industry Day

Exhibit-2014	Schuster, "Introducing the Microsoft Vista event log file format," *Digital Investigations* 4S (2007), S65-S75, Elsevier Ltd.
Exhibit-2015	"7.8. Packet Reassembly" from https://www.wireshark.org/docs/wsug_html_chunked/ChAdvReassemblySection.html
Exhibit-2016	Declaration of Jonathan Rogers
Exhibit-2017	Cisco webpage, Cisco ACNS Software Version 5.5, https://www.cisco.com/c/en/us/support/application-networking-services/acns-software-version-5-5/model.html
Exhibit-2018	Cisco webpage, Cisco ACNS Software Version 5.5 – Retirement Notification, https://www.cisco.com/c/en/us/obsolete/application-networking-services/cisco-acns-software-version-5-5.html
Exhibit-2019	Wikipedia – Maximum transmission unit, https://en.wikipedia.org/wiki/Maximum_transmission_unit
Exhibit-2020	Deposition Transcript of Dr. Kevin Jeffay in IPR2018-01512, taken on June 5, 2019
Exhibit-2021	Deposition Transcript of Eli Fuchs in IPR2018-01512, taken on June 28, 2019

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

This paper complies with the type-volume limitation of 37 C.F.R. § 42.24. The paper includes 13,956 words, excluding the parts of the paper exempted by § 42.24(a).

This paper also complies with the typeface requirements of 37 C.F.R. § 42.6(a)(ii) and the type style requirements of § 42.6(a)(iii)&(iv).

/James Hannah/

James Hannah (Reg. No. 56,369)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road,
Menlo Park, CA 94025
(650) 752-1700

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), that service was made on the Petitioner as detailed below.

Date of service	July 5, 2019
Manner of service	Electronic Mail (dmcdonald@merchantgould.com; jblake@merchantgould.com; kott@merchantgould.com; mwagner@merchantgould.com)
Documents served	PATENT OWNER'S RESPONSE
Persons Served	Daniel W. McDonald Jeffrey D. Blake Kathleen E. Ott Michael Wagner

/James Hannah/
James Hannah
Registration No. 56,369
Counsel for Patent Owner