Trials@uspto.gov
571-272-7822

Paper 8
Date Entered: March 20, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2018-01512
Patent 9,565,213 B2

Before BRIAN J. McNAMARA, STACEY G. WHITE, and JOHN P. PINKERTON, *Administrative Patent Judges.*

McNAMARA, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
35 U.S.C. § 314
37 C.F.R. § 42.4(a)

BACKGROUND

Cisco Systems, Inc. ("Petitioner") filed a Petition, Paper 1 ("Pet."), to institute an *inter partes* review of claims 1–16 (the "challenged claims") of U.S. Patent No. 9,565,213 B2 ("the '213 patent"). 35 U.S.C. § 311. Centripetal Networks, Inc. ("Patent Owner") timely filed a Preliminary Response, Paper 7 ("Prelim. Resp."), contending that the petition should be denied as to all challenged claims. We have jurisdiction under 37 C.F.R. § 42.4(a) and 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Having considered the arguments and the associated evidence presented in the Petition and the Preliminary Response, for the reasons described below, we institute *inter partes* review.

REAL PARTIES IN INTEREST

Petitioner identifies itself as the sole real party-in-interest. Pet. 1. Patent Owner identifies itself as the sole real party-in-interest. Paper 4, 1.

RELATED PROCEEDINGS

The Petition states that the '213 patent is asserted in the following litigation:

Centripetal Networks, Inc. v. Cisco Sys, Inc., 2:18-cv-00094-MSD-LRL, E.D. Va. (filed Feb. 13, 2018);

Centripetal Networks, Inc. v. Keysight Tech, Inc., 2:17-cv-00383-HCM-LRL, E.D. Va. (filed Jul. 20, 2017) (the "Keysight litigation").

The Petitioner also identifies the following proceeding concerning the '213 patent:

Cisco Systems, Inc. v. Centripetal Networks, Inc., Case IPR2018-01386 filed July 12, 2018. Pet. 1

THE ’213 PATENT (EXHIBIT 1001)

The ’213 patent discloses methods and systems for protecting a secured network. Ex. 1001, Abstract. Figure 1 of the ’213 patent is shown below:

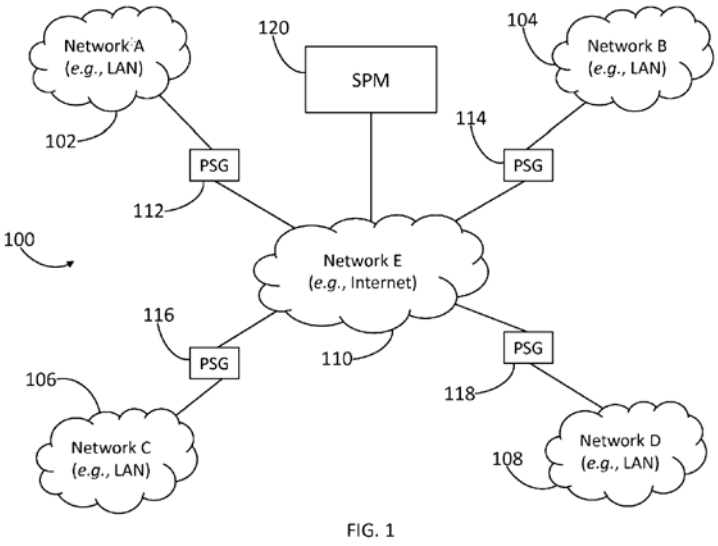


FIG. 1

Figure 1 illustrates a network environment that includes packet security gateways (PSGs) situated between networks and a security policy management (SPM) server that communicates dynamic security policies to the PSGs. *Id.* at 4:53–55, 4:66–5:3, Fig. 1. The PSGs perform packet transformation functions on received packets according to rules in a dynamic security policy that specifies one or more packet transformation functions that should be performed on packets associated with specific criteria. *Id.* at 7:7–13.

> The specified criteria may take the form of a five-tuple of values selected from packet header information, specifying a protocol

> type of the data section of the IP packet (e.g., TCP, UDP, ICMP, or any other protocol), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

Ex. 1001, 7:13–19, Fig. 3.

The '213 patent describes packet transformation functions that forward packets into the network (e.g., Ex. 1001, 2:50–52), drop packets (e.g., *id*. at 2:57–59), or perform functions other than forwarding or dropping the packets, (e.g., *id.* at 1:49–51). For example, rules in a dynamic security policy may specify a transformation function that routes or switches packets to a network address corresponding to a monitoring device by encapsulating the packet with a header that corresponds to the network address of the monitoring device. *Id.* at 11:14–33. The monitoring device strips the header and copies the packets, or data within the packets, for subsequent review before forwarding the packets to the destination address. *Id.* at 11:22–33.

Various combinations of rules may implement services, such as a network threat awareness service in which a packet transformation function produces a digest or log of the packet, "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." *Id.* at 11:36–54. Such packet logs can employ a logging standard, such as syslog, and be read by awareness application servers that perform transformations to produce awareness information that can be accessed by client applications. *Id*. at 54–60.

ILLUSTRATIVE CLAIM

Claim 1, reproduced below, is illustrative.

1. A method comprising:

receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;

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

identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application layer packet-header information;

performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises

identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;

generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and

reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and

routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.

Id. at 25:14–55.

ART CITED IN PETITIONER'S CHALLENGES

Petitioner cites the following references in its challenges to patentability:

Reference	Designation	Exhibit No.
Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5	ACNS	1008
U.S. Patent No. 9,172,627 B2	Kjendal	1009
"An Architecture for Differentiated Services," Network Working Group Request for Comments 2475, The Internet Society, Dec. 1998	Diffserv	1011

CHALLENGES ASSERTED IN PETITION

Claims	Statutory Basis	Challenge
1–9	35 U.S.C. § 103(a)	Obvious over ACNS in view of Kjendal
10–16	35 U.S.C. § 103(a)	Obvious over ACNS in view of Kjendal and Diffserv

ORDINARY SKILL IN THE ART

Noting that relevant experience and education can substitute for each other, Petitioner states that a person of ordinary skill in the relevant art on April 16, 2014 (the filing date of the application that matured in the '213 patent), would have had a bachelor's degree in computer science, computer engineering, or an equivalent, four years of professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack. Pet. 19 (citing Ex. 1004, Declaration of Dr. Kevin Jeffay ("Jeffay Decl.") ¶¶ 22–24). Petitioner's definition of a person of ordinary skill, which Patent Owner does not dispute, appears appropriate for the technology addressed by this proceeding.

CLAIM CONSTRUCTION

The Petition has been accorded a filing date of August 20, 2018. Paper 6. For petitions accorded a filing date before November 13, 2018, we interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). In applying a broadest reasonable construction, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Petitioner proposes the following claim constructions (Patent Owner does not propose constructions for any other terms):

Dynamic security policy. Petitioner proposes that "dynamic security policy" be construed 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." Pet. 14 (citing Ex. 1001, 4:58–63 (Ex. 1004, Jeffay Decl. ¶¶ 105–107). Petitioner further notes that the '213 patent describes "dynamic security policy" as being created either manually or automatically. *Id.* at 14 (citing Ex. 1001, 14–41–47, 14:56–15:5, Ex. 1004, Jaffay Decl. ¶ 105).

Patent Owner argues that Petitioner's proposed construction improperly reads the term "dynamic" out of the claim and is inconsistent with the construction adopted by the district court in the Keysight litigation. PO Resp. 6–7. Patent Owner proposes that "dynamic security policy" be construed to mean "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets." *Id.* at 6.

The language proposed by Petitioner follows exactly the disclosure in the '231 Specification that states "[a]s used herein, a dynamic security policy includes [Petitioner's proposed construction]." Ex. 1001, 4:59–63. We also note the Specification states "[o]ptionally, a dynamic security policy may further specify additional parameters as described herein." *Id.* at 4:63–65. Patent Owner points to no disclosure in the '213 Specification that gives any meaning to the term "non-static" in its proposed construction.

Nothing in Petitioner's proposed construction precludes a "dynamic security policy" from changing at any time.

In view of the disclosure in the '213 Specification, consistent with the '213 Specification we construe "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.*

Rule/rules. Petitioner proposes that the term "rule/rules" be construed to mean "part of a dynamic security policy" that "may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria." Pet. 14–15 (citing Ex. 1001, 6:11–12, 7:10–13; Ex. 1004, Jeffay Decl., ¶¶ 108–110). Patent Owner argues that Petitioner's construction is ambiguous because it introduces criteria and packet transformation functions into the construction. Prelim. Resp. 7–8. Patent Owner proposes that we apply the same construction the district court applied when construing a different patent (U.S. Patent No. 9,137,205) in the Keysight litigation, i.e., "a condition or set of conditions that when satisfied cause a specific function to occur." *Id.* at 7 (citing Ex. 2001, 21–22). Although "rule" is used throughout the '231 Specification, "rule" is not defined. The exemplary dynamic security policy of Figure 3 is illustrative of how "rule" is used in the '231 patent. Figure 3 shows Rules 1–5, each of which causes an action, i.e., a packet transformation (e.g. accepting, denying, or forwarding packets to a monitoring device), in response to a specific set of conditions specified by a five-tuple (e.g., protocol, source address, source port, destination address and port address).

It is not necessary to define "rule/rules" as part of a dynamic security policy because claims 1 and 10 explicitly recite that the dynamic security policy comprises a rule. What is less clear from the language and punctuation is whether claims 1 and 10 recite (a) that the dynamic security policy comprises (i) at least one rule specifying application-layer packet-header information and (ii) a packet transformation function comprising a packet digest logging function, or (b) that the dynamic security policy comprises at least one rule specifying both an application-layer packet header information and a packet transformation function comprising a packet digest logging function. In the context of an obviousness analysis for this Decision, we need not and do not resolve this issue, as the challenges to the claims do not turn on this distinction. Having considered the '213 Specification and the evidence currently of record, we adopt the construction used in the Keysight litigation and construe "rule/rules" to mean *a condition or set of conditions that when satisfied causes a specific function to occur*.

Security policy management server (SPM server). Petitioner cites the '213 patent as stating that a SPM Server "includes any computing device configured to communicate a dynamic security policy to a packet security gateway." Pet. 15 (citing Ex. 1001, 4:38–40). Patent Owner proposes the same construction, except that Patent Owner proposes to substitute the word "server" for "any computing device," as proposed by Petitioner. Prelim. Resp. 8 (citing Pet. 15, which acknowledges that the '213 patent discloses a server). We agree with Patent Owner. The term "any computing device" is so broad in this context that it has no clear meaning. We note, however, that the '213 patent states that it does not use term "server" in the same context as used in a client-server architecture, where a server responds to requests

from a client. Ex. 1001, 13:67–14:6. Instead, "server" in the context of the '213 patent (and the related '205 patent) refers to a computing device that performs the functions described in the '215 patent, but not necessarily in the response to client computer requests. *Id.* Recognizing that the '213 patent discloses any such computing device be configured as a server, we construe "security policy management server" to mean *a server configured to communicate a dynamic security policy to a packet gateway*.

Packet security gateway (PSG). Petitioner proposes that we construe "packet security gateway (PSG)" to mean "a gateway computer configured to receive packets and perform a packet transformation function on the packets," stating that this construction is consistent with that agreed to by Patent Owner in the Keysight litigation. Pet. 15. Petitioner cites the '213 patent as stating a "packet security gateway" "includes any computing device configured to receive packets and perform a packet transformation function on the packets." *Id*. (citing Ex. 1001, 4:48–50). Patent Owner does not oppose Petitioner's proposed construction. Prelim. Resp. 8. As the proposed construction appears consistent with the use of the term in the '213 patent, we construe "packet security gateway" to mean *a gateway computer configured to receive packets and perform a packet transformation function on the packets.*

Packet transformation function. Petitioner proposes that we construe "packet transformation function" to mean "an action taken upon a packet." Pet. 16–17. Petitioner notes that the '213 patent does not define this term explicitly, but describes a packet transformation function as an action taken on a packet, such as forwarding, dropping, routing, and queuing packets. *Id.* at 16 (citing Ex. 1001, 2:37–57, 8:8–14, 10:6–10, Fig. 3). Patent Owner

proposes that we construe this term to mean a "function that transforms one or more packets from one state to another." Prelim. Resp. 9.

Patent Owner raises several issues from the Keysight litigation. According to Patent Owner, the Petition's statement that Patent Owner attempted to exclude forwarding and dropping packets from the definition of the "packet transformation" in the Keysight litigation misrepresents Patent Owner's position, because Patent Owner's proposed construction did not include the language "such as forward or drop." *Id*. at 8. Patent Owner contends that, although it noted some of the asserted claims of the related '205 patent claimed packet transformation functions other than forwarding or dropping packets, Petitioner intentionally included those excluded functions in its claim term. *Id*. at 9. The '205 patent claims are not before us in this proceeding, and it is unclear from this record if the packet transformation function in any of the '205 patent claims included forwarding or dropping packets. It appears from this argument, however, that Patent Owner acknowledges it intended to exclude forwarding and dropping packets from the construction of "packet transformation function." In any case, the '213 patent states explicitly that under certain conditions a packet transformation function may forward packets into the network (e.g., Ex. 1001, 2:50–52), drop packets (e.g., *id*. at 2:57–59), or refer to "performing at least one packet transformation function other than forwarding or dropping the packets," (e.g., *id.* at 1:49–51).

Patent Owner's proposed construction of "packet transformation function" as a "function that transforms one or more packets from one state to another" uses a variation of the operative term "transform" to define itself. Patent Owner does not cite to any discussion in the '213 patent about the

state of a packet or what it means to transform a packet from one state to another. Thus, we are not persuaded that Patent Owner's proposed construction provides a meaningful construction of the term.

The '213 Specification states that a dynamic security policy "identifies a packet transformation function to be performed on packets corresponding to the specified criteria." Ex. 1001, 4:59–63. Above, we construed the term "rule" to mean "a condition or set of conditions that when satisfied causes a specific function to occur." Consistent with that construction of rule, we note that the '231 Specification refers to "a packet transformation function specified by one of the rules." Ex. 1001, 1:57–58, 7:7–.13. The '231 Specification states that a dynamic security policy may include a rule that forwards a packet to a packet transformation function (e.g., 6:15–19) and that the packet transformation function may perform a number of operations, such as: forwarding packets to the network or an IPsec stack; dropping packets or sending them to an infinite sink (e.g., *id.* at 6:19–31); routing packets to a network address corresponding to a monitoring device whose address may be different from the packet's destination network address, and encapsulating packets with an IP header specifying the address corresponding to the monitoring device (*id.* at 11:14–26); and producing a digest or log of the packet information (*id.* at 11:45–54). Thus, rules identify conditions that cause packet transformation functions to carry out specific operations that may differ depending upon the rule that applies to detected packet conditions.

In consideration of the above, we construe the term "packet transformation function" to mean *operations performed on a packet*.

Monitoring Device. Petitioner proposes that we construe "monitoring device" to mean a "device configured to copy (or store) packets or data contained within them." Pet. 17 (citing Ex. 1004, Jeffay Decl. ¶ 123). Petitioner notes that the '213 patent does not define "monitoring device" explicitly, but refers to such a device as storing packets or data within them for subsequent review or analysis, and states that the monitoring device may need to strip an encapsulating header from the packets or route them based on their destination address. *Id.* (citing Ex. 1001, 17:9–18). Patent Owner argues that Petitioner's proposed construction improperly restricts the term to a specific embodiment in the '213 Specification in which the monitoring device may be required to perform certain functions. Prelim. Resp. 9. Although Patent Owner objects to Petitioner's construction, Patent Owner does not propose an alternative construction.

Independent claims 1 and 10 recite the PSG routing on a packet-by-packet basis to a monitoring device corresponding to the application-layer packet-header information (claim 1) or corresponding to packet-identification criteria (claim 10) in response to performing the packet transformation (claim 1) or packet digest logging (claim 10) function. The claims recite the monitoring device used in the packet transformation or logging functions. The '213 Specification discusses a dynamic security policy that provides a multi-dimensional monitoring service. Ex. 1001, 15:38–41. In the context of a VoIP call, the Specification describes packet transformation function 218 as forwarding packets to monitoring device 608 that may copy or store the packets or data contained within them for subsequent review, e.g., by law enforcement, strip the encapsulation from them, and forward the packets without the encapsulating header to the

network. *Id.* at 16:54–17:21; *see also, id.* at 11:26–31 (discussing similar functions performed by the monitoring device in the context of logging). Patent Owner does not identify any other functions described in the '213 Specification that are performed by the monitoring device. *See, id*. at 9–10.

In consideration of the above, we adopt Petitioner's construction as consistent with the '213 Specification and construe the term "monitoring device" to mean *a device configured to copy (or store) packets or data contained within them*.

ANALYSIS OF PETITIONER'S PRIOR ART CHALLENGES

Introduction

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc*., 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Claims 1–9 As Obvious Over ACNS in View of Kjendal

ACNS

The Cisco Application and Content Networking System (ACNS) is a "software solution" for "setting up and managing content delivery and content caching services in a centrally managed environment." Ex. 1008,

25, 1-1[1]. An ACNS device can be configured to operate in one of the following modes: (i) Content Distribution Manager, (ii) Content Engine; (iii) Content Router or (iv) IP/TV Program Manager. *Id.* at 1-2. All ACNS devices are shipped from the factory as Content Engines and must be reconfigured to operate in other modes. Ex. 1008, 2-14. Initial set-up requires (i) enabling a Content Distribution Manager using an interactive setup utility or device mode global configuration in the Command Line Interface (CLI), (ii) enabling a Content Engine as a centrally managed device, and, (iii) if content routing will be used to route requests, enabling a Content Router. *Id.* at 1-2, 2-3, 2-6–7, Fig. 2-1.

"The primary role of a Content Distribution Manager is to perform centralized content and device management . . . the Content Distribution Manager manages both content acquisition and distribution and also manages policy setting and configurations on individual Content Engines." *Id.* at 1-2. "Through the Content Distribution Manager GUI (Graphical User Interface), the network administrator can specify what content is to be distributed and to whom." *Id.* Petitioner analogizes the Content Distribution Manager to the claimed security policy management server ("SPM server" or "SPMS"). Pet. 20.

An ACNS Content Engine is "an 'in-line' device between end users and the Internet" that intercepts end user content requests, enforces policies to assure security and budgetary objectives are met, and can be used to "authenticate, monitor, log, and control web access from end users to

[1] Consistent with the Petition, we number the pages of the exhibits using the pagination printed in the original document, rather than the sequential page number of the exhibit. Pet. 19.

implement corporate policies regarding work environment and system security." Ex. 1008, 1-9. Among other tasks, upon receipt of a content request, an ACNS Content Engine "[p]asses the request through 'rules,' which might rewrite certain headers, redirect the request, or otherwise manipulate the request." *Id*. at 1-9–10. "Content Engines can be centrally managed through the Content Distribution Manager or locally as separate standalone content caches." *Id.* at 1-2. Petitioner analogizes the Content Engine to the claimed packet security gateway ("PSG").

Content Routers "redirect client requests to the closest Content Engine containing the content" using "the Domain Name System (DNS) to ensure that the Content Router receives all requests for content." Ex. 1008, 1-2.

IP/TV Program Managers are used by a system administrator "to set up and manage IP/TV scheduled or on-demand programs, channels, recording, and file transfers among IP/TV Servers." *Id.* at 1-3.

Petitioner contends that ACNS Content Engines perform packet transformation functions, citing the description of Configuring Caching Services so that a Content Engine need not retrieve the same data multiple times. Pet. 23 (citing Ex. 1008, 8-1). According to Petitioner, based on the user's HTTP request packet for information, ACNS determines whether the system is configured to allow the specific HTTP request method in the request packet, whether the system already has the information cached, and generating a log entry for the request. *Id.* (citing Ex. 1008, 8-23–24, disclosing that Content Engines accept or reject HTTP requests depending on whether the HTTP method is supported and that in HTTP 1.1 some request methods (e.g., GET, HEAD, or POST) are supported by default, a list of unsupported methods is maintained, and methods can be added to a

list of supported methods the Creating New HTTP Method for Content Engine window).

ACNS also discloses that administrators can maintain in various formats transaction logs of the date and time of a request, the URL requested, whether there was a cache hit or miss, the type of request, the number of bytes transferred, and the source IP address. See Ex. 1008, 19-1. Content Engines can send for logging only transactions associated with HTTP request authentication failures, or send all the transactions. *Id.* at 19–21.

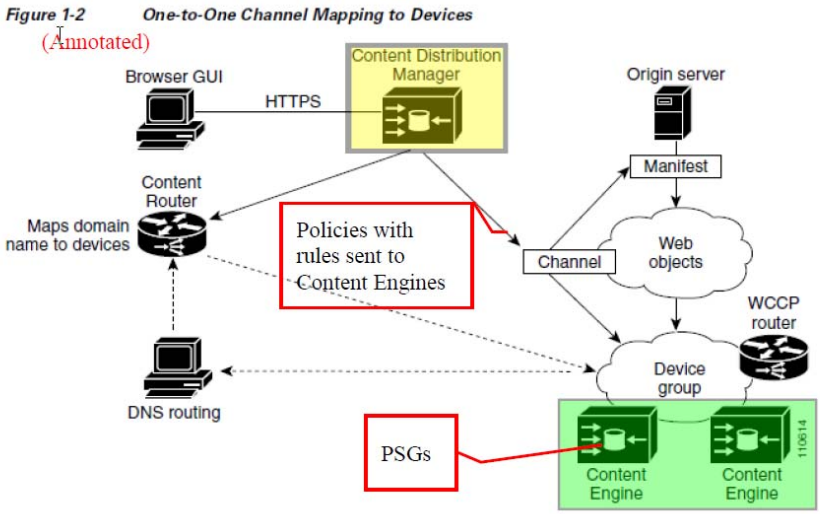
Kjendal

Petitioner states that Kjendal "relates to monitoring traffic for analysis and security by sending copies of certain, identified packets to a monitoring or logging device, based on policies provided to the device." Pet. 24 (citing Ex. 1009, Abstract). Kjendal discloses a system in which network policies are defined and regulated through an administrator controlled network policy server device that transmits established policies to network interface devices known as packet forwarding devices. Ex. 1009, 2:59–66. Kjendal discloses, either selectively or on a regular basis, mirroring one or more packets or portions of packets to a destination other than the original intended destination as part of determining the application associated with a flow or session being established. *Id.* at 3:43–60. Kenjdal also discloses dynamic mirroring is not limited to facilitating the identification of computer applications running on a network. *Id.* at 8:59–61.

Elements of Claim 1

Claim Element 1.1

Petitioner identifies as claim element 1.1 the limitation that recites "receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information." Pet. 25. Petitioner's annotated version of Figure 1-2 of ACNS is reproduced below:



Pet. 26. Petitioner's annotated drawing identifies the ACNS Content Distribution Manager as corresponding to the claimed SPM transmitting policies with rules to Content Engines that correspond to the claimed PSGs. *Id.* at 26–27. Petitioner contends that ACNS discloses at least two examples of "rules specifying application packet-layer information" that are part of a dynamic security policy provisioned to the Content Engines. *Id.* at 28. Citing the description in ACNS of Content Engines identifying HTTP packets and request methods associated with those packets and the ability to modify acceptable request methods, Petitioner contends that the rule is

"dynamic." *Id.*at 28 (citing Ex. 1008, 8-23; Ex. 1004 ¶¶ 155–157). Petitioner also cites the use of the ACNS Content Distribution Manager GUI to set up Internet Content Adaption Protocol (ICAP) rules for packet identification and field substitution as evidence in ACNS of rules specifying application-layer packet-header information in a dynamic policy provisioned by the Content Distribution Manager to the Content Engines. *Id.* at 29–30. Petitioner notes that, in ACNS, Content Engines can use ICAP based servers to implement rules to identify specific HTTP application layer packets and examine, filter, and modify fields with a substitution string, or re-route the HTTP packet, i.e. to transform application layer packets. *Id.* at 29 (citing Ex. 1008, 16-13–23; Ex. 1004 Jeffay Dec. ¶ 158).

Patent Owner contends that ACNS in view of Kjendal does not disclose "receiving a dynamic security policy from a security policy management server." Prelim. Resp. 16. Patent Owner argues that "the Content Distribution Manager is not concerned with network security and does not provide the claimed dynamic security policies to the Content Engine, which Petitioner alleges correspond to the claimed PSGs." Prelim. Resp. 16 (citing Ex. 1008, 38). We note, however, that ACNS explicitly states that one of the tasks of the Content Engine is "to implement corporate policies regarding work environment and system security." Ex. 1008, 1-9.

Patent Owner also argues that the Content Engines do not receive any policies from the Content Distribution Manager, because the CDM can only manage settings for pre-existing policies already installed on the Content Engines. Prelim. Resp. 17. Patent Owner asserts that Petitioner's statement that dynamic security policies are generated at the CDM based on user input is misleading. *Id*. at 18 (citing Pet. 27).

Chapter 2 of ACNS discusses initial configuration. As noted above, all ACNS devices are factory shipped as Content Engines. Ex. 1008, 2-6, 2-14. The first initialization step is to enable a device as the CDM using either a setup utility or by accessing the device command line interface (CLI) through a console or Telnet session. *Id*. at 2-14, 2-16, Fig. 2-1. The administrator can then use the Quick Start tool to "select a set of content engines and provision them for caching, streaming, and pre-positioning using a small subset of options," with advanced option available from the main user interface. *Id.* at 2-12–13. As a security feature to prevent unauthorized devices from joining a network, administrators who choose not to use the Quick Start tool must activate devices in the Content Distribution Manager GUI. *Id.* at 2-22. The Content Distribution Manager GUI includes tabs to access CDM functionality for configuring and managing devices, services, and system features of the network and navigation bars providing menus for each tab that allow a user to create new elements or add existing elements. *Id.* at 3-4–5. For example, Cisco provides a web circuit communication protocol (WCCP) in which a WCCP enabled router is configured in the interface between the Internet and a Content Engine to direct a content request to a Content Engine containing the content. *Id*. at 4-2–3. To use this feature, an administrator must configure the Content Engine properly (*id.* at 4-7–4-10) and configure four sets of services to configure WCCP services (*id*. at 4-10–4-14). In each case, the ACNS instructs the administrator to choose the "Devices" tab on the CDM menu and "[c]lick to the **Edit** icon next to the Content Engine for which you want to configure WCCP (general or service) settings." *Id.* at 4-7, 10. The administrator's selection of the "Edit" icon to configure the device is merely

an expedient that allows the administrator to configure a content engine activated on the network.

Petitioner cites examples that concern how HTTP caching services are configured. *See generally*, Ex. 1008, Chapter 8. ACNS describes how to use the CDM GUI to configure HTTP connection settings, e.g., by entering port numbers from which the Content Engine may receive requests (Ex. 1008, 8-2–5) and by entering HTTP caching parameters for caching HTTP requests (*id*. at 8-6–9).

ACNS discloses that Content Engines service protocols for which they are configured. *Id.* at 8-2. In addition, Content Engines accept or reject an HTTP request depending on whether the HTTP request method is supported. *Id.* at 8-23. That some methods are supported by default does not change the fact that ACNS teaches the administrator configures an active Content Engine either initially or at a later time by clicking the "Edit" icon next to the name of the corresponding Content Engine on the CDM GUI to add other HTTP request methods to the selected Content Engine. *Id.* at 8-23–24. Thus, the administrator customizes the rules implemented in the Content Engines. To the extent an administrator manipulates settings, such as port numbers and HTTP request methods accepted by the Content Engine, such manipulation is the result of externalities, such as HTTP standards. It is the administrator who, through the Content Distribution Manager, configures the performance of a Content Engine in the context of such externalities.

In consideration of the above, for purposes of institution we are not persuaded by Patent Owner's arguments that ACNS teaches only managing settings for pre-existing policies. For purposes of institution, we are

persuaded that Petitioner has demonstrated the combination of ACNS and Kjendal discloses this claim element.

Claim Element 1.2

Petitioner identifies as claim element 1.2 the limitation that recites "a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information." Petitioner cites ACNS as teaching packet transformation functions that include logging all packets or only some packets and, through a user interface, allowing a user to choose to log and to configure ACNS transaction logging functionality with a single policy to be sent from the Content Distribution manager to one or more Content Engines. Pet. 31–34.

Petitioner acknowledges that "ACNS does not explicitly state that its packet digest logging functions are performed on packets based on their meeting criteria in the two application-layer packet-header rules discussed above in element [1.1]," i.e., application-layer packet-header information identified by the HTTP request method or ICAP rules. *Id*. at 30–31 (citing Ex. 1004, Jeffay Dec. ¶ 165), 35. Instead, Petitioner cites Kjendal as disclosing "a system where application-layer packet-header information is used to determine what should be logged, noting that Kjendal teaches 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 application types. *Id.* at 31 (citing Ex. 1004, Jeffay Decl. ¶¶ 164–167), 35 (citing Ex. 1009, 10:23–33). Petitioner argues that, recognizing ACNS discloses an administrator can perform real time transaction logging by sending only logs of HTTP authentication failures to the syslog server rather than logs of all transactions, a person of ordinary

skill would understand that an administrator could selectively log other types of transaction information, as taught by Kjendal. *Id.* at 36–37. Thus, according to Petitioner, "given the teachings of Kjendal and ACNS, it would have been obvious to a POSA to implement the ACNS system such that the logging function logs packets based on application-layer packet-header rules." *Id.* at 31.

Patent Owner contends that by "improperly "divorc[ing] the claimed 'dynamic security policy that comprises a rule specifying' from 'a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information,'" Petitioner attempts to demonstrate that a packet digest logging function is obvious without demonstrating that the packet digest logging function is part of a dynamic security policy." Prelim. Resp. 20–21. Patent Owner points out that the ACNS Transaction Logs are unrelated to the HTTP Method policy that Petitioner alleges the Content Engines receive as a dynamic security policy from the Content Distribution Manager. *Id.* at 22. Patent Owner explains that because ACNS transaction logging is applied to all HTTP requests or only those HTTP requests for which authentication fails, ACNS does not suggest the packet logging function is performed on packets having the application-layer packet-information information or that it is part of a dynamic security policy received from the Content Distribution Manager. *Id.* at 22–24. Patent Owner contends that simply sending a copy of a packet to a device called a network logger is not a packet digest logging function as claimed because that function requires other features recited in the claims. *Id.* at 26. Therefore, according to Patent

Owner, even the combination of ACNS and Kjendal does not teach the claimed subject matter. *Id.*

As discussed above Petitioner acknowledges that ACNS lacks the specific teachings Petitioner cites in Kjendal and, instead, argues that a person of ordinary skill would apply the teachings of Kjendal to log other types of data as taught by ACNS. As Petitioner relies upon the combination of ACNS and Kjendal to teach all the elements of the claims, we are not persuaded by Patent Owner's arguments concerning claim element 1.2 because they do not fully address what one of ordinary skill in the art would have learned from the combination and thus, we address the remaining clam elements below.

Claim Element 1.3

Petitioner identifies as claim element 1.3 the limitation that recites "receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway." Pet. 37. Petitioner cites the transmission of streaming media, as illustrated in Fig. 9-1 of ACNS, as disclosing Content Engines analogous to the claimed PSGs that receive packets associated with a network behind and protected by the Content Engines. Pet. 37–38. Petitioner also cites ACNS as disclosing the ability of a user to view Content Engine statistics, including the number of packets sent and received. *Id.* at 39 (citing Ex. 1008, 21-14–18; Ex. 1004, Jeffay Decl. ¶ 171).

Patent Owner contends that Petitioner has not demonstrated that ACNS in view of Kjendal discloses receiving packets associated with a network protected by a packet security gateway. Prelim. Resp. 26. Patent Owner argues that Petitioner "relies on one oblique reference in ACNS that

states the Content Engine protects a network." *Id.* (citing Pet. 38). Patent Owner further notes that, although ACNs mentions preventing viruses by communicating with an ICAP server, the Content Engine does not provide that functionality and there is no teaching that the Content Engine protects the network using a dynamic security policy. *Id.* at 27.

As discussed above, ACNS explicitly states""[c]ontent caching, filtering, and access control services address the need to . . . authenticate, monitor, log, and control web access from end users to implement corporate work environment and system security." Ex. 1004, 1-9. ACNS further states Content Engines, which are placed "at the network edge where the corporate network interfaces with the Internet," can "intercept content requests made by end users and enforce the above policies" and that Content Engine "[p]asses the request through 'rules,' which might rewrite certain headers, redirect the request, or otherwise manipulate the request." *Id.* at 1-9–10. Thus, we are not persuaded by Patent Owner's argument concerning claim element 1-3. For purposes of institution, we are persuaded that Petitioner has demonstrated the combination of ACNS and Kjendal teaches this claim element.

Claim Element 1.4

Petitioner identifies as claim element 1.4 the limitation that recites "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." Pet. 39. Petitioner cites ACNS as disclosing Content Engines examining the application-layer packet-headers of HTTP packets to determine if the HTTP request method is

supported by the Content Engine. Pet. 39–40. Petitioner also cites the disclosure in ACNS that a Content Engine examines packet-header information using ICAP rules to identify packets and the rule actions to apply. *Id.* at 40. Patent Owner does not discuss this limitation explicitly. For purposes of institution, we are persuaded that Petitioner has demonstrated the combination of ACNS and Kjendal teaches this claim element.

Claim Element 1.5

Petitioner identifies as claim element 1.5 the limitation that recites "performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises." Pet. 41. Petitioner cites ACNS as performing packet transformations, e.g., (i) allowing or denying packets based on included HTTP request methods, and (ii) a packet digest logging function to notify the Content Engine to extract and log defined information from the packet header. Pet. 41 (citing Ex. 1008, 8-23, 19-1– 5). Petitioner states that a person of ordinary skill would understand that the ACNS system performs such transformations on a packet-by-packet basis to avoid skipping packets, thereby avoiding invalid packets. *Id*. (citing Ex. 1004, Jeffay Decl. ¶ 177). Patent Owner does not discuss this claim element explicitly. For purposes of institution, we are persuaded that Petitioner has demonstrated the combination of ACNS and Kjendal teaches this claim element.

Claim Element 1.6

Petitioner identifies as claim element 1.6 the limitation that recites "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." Pet. 42. Petitioner cites ACNS as disclosing the existence of multiple information logging formats that may include a subset of information from the application-layer packet-header. *Id*. (citing Ex. 1008, 19-1, discussing a "squid" log entry). Petitioner asserts that a person of ordinary skill would have known that such information as the URL an HTTP method are found in the header of an HTTP application-layer packet and that any subset of the information from the packet could be logged. *Id*. (citing Ex. 1004, Jeffay Decl. ¶181). Patent Owner does not discuss this claim element explicitly. For purposes of institution, we are persuaded that Petitioner has demonstrated the combination of ACNS and Kjendal teaches this claim element.

Claim Element 1.7

Petitioner identifies as claim element 1.7 the limitation that 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." Pet. 43. Petitioner cites the "squid" log entry in ACNS as the default format for transaction logging in the Content Engine. *Id.* at 43–44, (citing Ex. 1008, 19-1). ACNS states that typical transaction log fields include "the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of bytes transferred, and the source IP address." Ex. 1008, 19-1. Petitioner notes

that the ACNS system identifies and extracts application packet information and combines information not found therein to generate an internal record before writing it in the specified format. Pet. 44 (citing Ex. 1008, 19-1–5). Patent Owner does not discuss this claim element explicitly. For purposes of institution, we are persuaded that Petitioner has demonstrated the combination of ACNS and Kjendal teaches this claim element.

Claim Elements 1.8 and 1.9

Petitioner identifies as claim element 1.8 the limitation that recites "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." Pet. 44.

Petitioner identifies as claim element 1.9 the limitation that recites "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." Pet. 45.

As to claim element 1.8, Petitioner notes that "ACNS also teaches that the subset of information, already formatted in one log format, may be reformatted into syslog format." *Id.* at 44 (citing Ex. 1004 ¶¶186-187, Ex. 1008, 19-19–21). As to claim element 1.9, Petitioner cites Kjendal as teaching routing identified packets to a monitoring device based on rules by mirroring selected packets to a wide variety of logger devices that perform analysis, identification, and decryption based on application-layer packet header information. *Id.* at 45–46.

Patent Owner contends that Petitioner has failed to demonstrate that ACNS in view of Kjendal discloses routing packets corresponding to the packet identification criteria to a monitoring device in response to performing a logging function. Prelim. Resp. 28. Patent Owner argues that Kjendal fails to teach this limitation because Kjendal discloses mirroring packets without disrupting the original data flow. *Id.* As discussed above, ACNS discloses Content Engines that can intercept content requests and pass the requests through rules that rewrite headers or redirect the request. Ex. 1004, 1-9–10. Thus, on this record we are persuaded that ACNS suggests the ability to reroute requests. We further note that claim 1 does not recite diverting packets to a monitoring device to the exclusion of the original destination. Claim element 1.9 recites only that the packets be routed to a monitoring device and does not exclude mirroring.

Patent Owner also argues that Kjendal describes mirroring "**before** identifying any application data, let alone application-layer packet header-information." Prelim. Resp. 29 (citing Ex. 1009, 7:43–49). Petitioner argues Kjendal discloses "a system where application-layer packet-header information is used to determine what should be logged, noting that Kjendal teaches 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 application types. Pet. 31 (citing Ex. 1004, Jeffay Decl. ¶¶ 164–167), 35 (citing Ex. 1009, 10:23–33). Kjendal discloses that the set-up, teardown, and filtering employed in mirroring activity can be adjusted based on network policies and that the criteria for mirroring may include frames of packets, the content of particular fields in a frame, flow counts, the end of a flow, regularly timed mirroring, or any other conditions of interest

to the network administrator. Ex. 1009, 9:63–10:9. In view of these disclosures, we are not persuaded by Patent Owner's arguments and determine that, for purposes of institution, Petitioner has demonstrated that the combination of ACNS and Kjendal would have suggested claim elements 1.8 and 1.9 to a person of ordinary skill.

Motivation To Combine Teachings of ACNS and Kjendal

Noting that port-mirroring was deployed routinely on Cisco router systems, Petitioner contends that a person of ordinary skill would have found it obvious and straightforward to incorporate the specific packet monitoring teachings of Kjendal with the teachings of ACNS, including ACNS's teaching of selecting on a packet-by-packet basis those packets comprising selected application-layer packet header information. Pet. 25.

Patent Owner responds that whether or not port-mirroring was well known, Petitioner has not demonstrated a reason a person of ordinary skill would implement port-mirroring with ACNS. Prelim. Resp. 30. According to Patent Owner, Petitioner's statement that Kjendal discloses a system where application layer information is used to determine what should be logged mischaracterizes Kjendal, because there is no evidence of what occurs at the network logger, or that the rules specify a packet digest logging function to be performed upon matching application-layer packet-header information. *Id*. at 30–31. We are not persuaded by Patent Owner's argument. Kjendal states

> Multiple criteria are established for what, and where to mirror the traffic. The criteria include what frames of traffic to mirror, one or more portions of the selected frames to mirror, one or more portals through which to mirror the selected frames, destination for the mirroring and the establishment of a mirror in a device to carry out the mirroring.

Ex. 1009, Abstract.

Patent Owner further argues that ACNS does not need to perform a mirroring function to view network traffic at the Content Engine because it already logs packets. Prelim. Resp. 31 (citing Ex. 1008, 19-1[2]). Petitioner cites ACNS for that same proposition. *See, e.g.,* Pet. 23, 31–34. Petitioner argues that, recognizing ACNS discloses an administrator can perform real time transaction logging by sending only logs of HTTP authentication failures to the syslog server rather than logs of all transactions, in view of Kjendal's teachings, a person of ordinary skill would understand that an administrator could selectively log other types of transaction information. *Id.* at 36–37.

In consideration of the above, we are persuaded for purposes of this Decision that Petitioner has cited sufficient evidence to demonstrate that a person of ordinary skill would have been motivated to combine the teachings of ACNS and Kjendal.

Conclusion As To Claim 1

For the reasons discussed above, we are persuaded that, for purposes of institution, Petitioner has demonstrated that a person of ordinary skill would have been motivated to combine ACNS and Kjendal and that the combined teachings of the references teaches or at least suggests all of the features recited in claim 1. Therefore, we are persuaded that, for purposes of institution, Petitioner has demonstrated a reasonable likelihood it will prevail in its challenge to claim 1.

[2] Patent Owner cites Ex. 1008, 19-1 as Ex. 1008, 697 (using the sequential page number of Ex. 1008)

Claim 2

Claim 2 depends from claim 1 and recites "the at least one rule indicates performing an accept packet transformation function on the packets comprising the application-layer packet-header information, and wherein the performing the packet transformation function comprises forwarding, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information toward its respective destination." Noting that ACNS Content Engines accept (or reject) an HTTP request depending upon whether the HTTP request is supported, Petitioner argues that a person of ordinary skill would understand that the HTTP packet will be accepted based on HTTP (application layer) request method (packet header) information and forwarded to its destination. Pet. 47–48 (citing Ex. 1008, 8-23, Ex. 1004, Jeffay Decl. ¶¶ 199–201). Petitioner also notes that ACNS discloses the Content Engine may function as a forward proxy that receives user requests and either responds to the request of forwards the request to an outside server to obtain the requested content. *Id.* (citing Ex. 1008, 1-3).

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 2 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 2.

Claim 3

Claim 3 depends from claim 1 and recites "the at least one rule indicates performing a deny packet transformation function on the packets

comprising the application layer packet-header information, and wherein the performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet header information." Petitioner notes that, in a manner similar to HTTP packet acceptance discussed with respect to claim 2, ACNS a person of ordinary skill would understand that an ACNS Content Engine could reject an HTTP packet based on the Request Method. Pet. 49.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 3 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 3.

Claim 4

Claim 4 depends from claim 1 and recites "the application-layer packet-header information identifies one or more hypertext transfer protocol (HTTP) packets, and wherein identifying the one or more packets comprising the application-layer packet-header information comprises determining by the packet security gateway that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets." Petitioner notes that, as discussed above, ACNS Content Engines can accept or reject an HTTP request depending upon whether the HTTP request method is supported. Pet. 50.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has

demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 4 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 4.

Claim 5

Claim 5 depends from claim 4 and recites "the one or more HTTP packets comprise an HTTP GET method call, and wherein determining that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets comprises determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP GET method call." As Petitioner points out ACNS discloses the HTTP GET method call among rule criteria and that the logging system identifies the Request Method (including GET) in order to create a corresponding log entry. Pet. 51.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 5 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 5.

Claim 6

Claim 6 depends from claim 5 and recites "the HTTP GET method call specifies a uniform resource identifier (URI), and wherein determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP GET method call comprises determining that the one or more packets comprising the application-layer packet-header information originated from or are destined for a network

address corresponding to the URI." Petitioner notes that "ACNS teaches implementing URL filtering for HTTP packets containing a Request Method, such as GET, based on the URI contained within the HTTP (application-layer) packet-header." Pet. 52 (citing Ex. 1008, 16-2525–33, Ex. 1004, Jeffay Decl. ¶215). Petitioner also cites the "squid" log format example in which the log comprises a "peerhost" field to demonstrate whether the packet is being forwarded to the URI or another address. *Id*. at 53 (citing Ex. 1008, 19-1–8; Ex. 1004, Jeffay Decl. ¶ 218).

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 6 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 6.

Claim 7

Claim 7 depends from claim 4 and recites "the one or more HTTP packets comprise an HTTP PUT method call, and wherein determining that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets comprises determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP PUT method call." Petitioner notes that the HTTP 1.1 specification discussed in ACNS includes eight Request Methods, including PUT. Pet. 54.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has

demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 7 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 7.

Claim 8

Claim 8 depends from claim 7 and recites "the HTTP PUT method call specifies a uniform resource identifier (URI), and wherein determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP PUT method call comprises determining that the one or more packets comprising the application-layer packet-header information originated from or are destined for a network address corresponding to the URI." Petitioner argues that ACNS discloses this feature for the same reasons as those discussed with respect to claims 6 and 7. Pet. 54–55.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 8 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 8.

Claim 9

Claim 9 depends from claim 1 and recites "the at least one rule comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one or more packets comprising the application-layer packet-header information comprises determining by the packet security gateway that each of the one

or more packets comprising the application-layer packet-header information corresponds to at least one of the one or more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports." Petitioner notes that the five-tuple of protocol, source address, destination address, source port, and destination port as identification criteria is well known. Pet. 55–56 (citing Ex. 1004, Jeffay Decl. ¶¶ 231–232). Petitioner cites Chapter 17 of ACNS as teaching filtering packets using Access Control Lists based on all five-tuple elements. *Id.* at 56 (citing Ex. 1008, Table 17-4).

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 9 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 9.

Claims 10–16 As Obvious Over ACNS In View of Kjendal and Diffserv

Motivation To Combine Diffserv With ACNS and Kjendal

Petitioner describes differentiated services as allowing a system to give certain packets priority over others. Pet. 59 (citing Ex. 1004, Jeffay Decl. ¶¶ 68–71). According to Petitioner "Diffserv is a flexible standard for marking each network packet with a priority value within the DSCP (Differential Service Code Point) field." *Id.* (citing Ex. 1011, §§ 2, 2.31). Petitioner cites the description in ACNS of implementing differentiated services that utilize a DSCP selector, and a differentiated management

services screen referring to Quality of Service (QoS), noting that ACNS uses DSCP values carried in packet headers to enable Content Engines to classify packets bases on quality of service differentiation. *Id.* at 59–61. Petitioner contends that a person of ordinary skill would have recognized DSCP based packet filtering packet as an obvious variant, as filtering can be based on any network packet filed. *Id.* at 61–62. Petitioner also notes that Kjendal teaches mirroring with network services including QoS. *Id.* at 62 (citing Ex. 1009, 2:14–16, 3:1–7).

Patent Owner does not respond to Petitioner's contentions concerning the motivation to combine the teachings of ACNS and Kjendal with Diffserv. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that a person of ordinary skill would have been motivated to combine the teachings of ACNS, Kjendal, and Diffserv, as proposed by Petitioner.

Claim 10

As Petitioner notes, claim 10 is similar to claim 1, except that where claim 1 recites the dynamic security policy comprises at least one rule specifying application-layer packet-header information, claim 10 broadly recites that the rule includes packet-identification criteria. Pet. 62. Claim 10 also recites that the packet-identification criteria comprises a Differential Service Code Point (DSCP) selector (identified by Petitioner as claim element 10-3). Petitioner cites Diffserv as disclosing a system that may select packets in a traffic stream based on the content of some portion of the packet header, specifically the DSCP information. *Id.* at 63. Petitioner further notes that ACNS contemplates a combination with Diffserv because ACNS teaches the presence of the DSCP field in packets and implementing

QoS based on the DSCP field. *Id.* at 66 (citing Ex. 1008, 17-1–8; Ex. 1004, Jeffay Decl. ¶ 263). Thus, Petitioner argues that the combination of ACNS, Kjendal, and Diffserv teaches the claimed elements of claim 10, including classifier rules that include the claimed packet-identification criteria. *Id.* at 63.

Patent Owner contends that the combination of ACNS, Kjendal, and Diffserv does not teach the elements of claim 10 for the same reasons that ACNS and Kjendal fail to teach the elements of claim 1. Prelim. Resp. 32–34. For purposes of institution, we were not persuaded by Patent Owner's arguments concerning claim 1. In the absence of further evidence at this stage of the proceeding, we are persuaded that Petitioner has demonstrated a reasonable likelihood it will prevail in its challenge to claim 10 based on the combination of ACNS, Kjendal, and Diffserv.

Claim 11

Claim 11 depends from claim 1 and further recites "the subset of information comprises at least one of a portion of data from the packet, a source address of the packet, a source port of the packet, a destination address of the packet, a destination port of the packet, a transport-protocol type of the packet, a uniform resource identifier (URI) from the packet, an arrival time of the packet, a size of the packet, a flow direction of the packet, an identifier of an interface of the packet security gateway that received the packet, or one or more media access control (MAC) addresses associated with the packet." Petitioner cites ACNS as disclosing a Content Engine that may identify several of the claimed criteria from individual packets including that date and time a request was made, the URL that was requested, the number of bytes transferred and the source IP address. Pet.

69–70. Petitioner cites Diffserv as teaching specific information that should be gathered for a log record, including the date/time the packet was received and the destination and IP address. *Id.* at 70.

Patent Owner does not respond to Petitioner's contentions. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 11 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 11.

Claim 12

Claim 12 depends from claim 10 and further recites "temporarily storing data in a memory of the packet security gateway, the data comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and utilizing, by the packet security gateway, the data to generate a message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria." Noting that ACNS discloses real time transaction logging and an example of a real-time syslog message sent from the transaction logging module (Content Engine) to the remote syslog host, Petitioner argues that ACNS teaches the message is generated and thus temporarily stored in memory at the Content Engine (analogous to the claimed PSG) as an obvious step before sending messages. Pet. 71 (citing Ex. 1008, 19-19; Ex. 1004, Jeffay Decl., ¶ 290).

Patent Owner does not respond to Petitioner's contentions. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv

discloses the features recited in claim 12 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 12.

Claim 13

Claim 13 depends from claim 12 and recites "communicating, by the packet security gateway and to the security policy management server, the message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet identification criteria." Noting that ACNS provides instruction for configuring the destination of the syslog messages, Petitioner contends that a person of ordinary skill would understand that one likely location for the syslog server that receives log messages is the Content Distribution Module (corresponding to the claimed SPM). Pet. 72 (citing Ex. 1008, 19-20–21; Ex. 1004, Jeffay Decl. ¶ 294).

Patent Owner does not respond to Petitioner's contentions. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 13 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 13.

Claim 14

Claim 14 depends from claim 10 and recites "reformatting the subset of information specified by the packet digest logging function in accordance with the logging system standard comprises reformatting the subset of information specified by the packet digest logging function in accordance with a syslog logging system standard."

Noting that the ’213 patent acknowledges logging can be implements using a known standard, e.g., Syslog, Petitioner cites ACNS as reformatting information into the syslog system standard. Pet. 73.

Patent Owner does not respond to Petitioner’s contentions. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 14 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 14.

Claim 15

Claim 15 depends from claim 10 and recites “the packet-identification criteria comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria corresponds to at least one of the one or more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports.”

Petitioner notes that, except for referring to the packet identification of the rule, claim 15 is functionally equivalent to claim 9 discussed above. Pet. 73–74. Petitioner argues that the references disclose the elements of claim 15 for the same reason they disclose the elements of claim 9. *Id.*

Patent Owner does not respond to Petitioner's contentions concerning claim 9 or claim 15. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 15 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 15.

Claim 16

Claim 16 depends from claim 10 and recites "the packet-identification criteria comprises application-layer packet-header information, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria comprises at least a portion of the application-layer packet-header information." Petitioner contends that the analysis discussed above in the context of claim elements 1.1 and 1.4 applies equally to claim 16. Pet. 74–75.

Patent Owner does not respond to Petitioner's contentions. Based on the foregoing, we are persuaded that for purposes of institution, Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 16 and that Petitioner has shown a reasonable likelihood it will prevail in its challenge to claim 16.

SUMMARY

For the reason discussed above, with respect to claims 1–9, we are persuaded that, based on the current record, Petitioner has demonstrated that a person of ordinary skill would have been motivated to combine the teachings of ACNS and Kjendal and that this combination of references

teaches or at least suggests all the elements of claim 1–9. We are also persuaded that, with respect to claims 10–16, Petitioner has demonstrated that a person of ordinary skill would have been motivated to combine the teachings of ACNS, Kjendal, and Diffserv and that this combination of references teaches all the elements of claims 1–10. Thus, we are persuaded that Petitioner has demonstrated a reasonable likelihood it will prevail on all of its challenges to claims 1–16.

ORDER

In consideration of the foregoing, it is hereby:

ORDERED that pursuant to 35 U.S.C. § 314(a) an *inter partes* review of the '213 Patent is hereby instituted, commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

FURTHER ORDERED that the trial is authorized on all grounds set forth in the Petition, in particular:

Claim 1–9 as obvious under 35 U.S.C. § 103(a) over ACNS in view of Kjendal; and

Claims 10–16 as obvious under 35 U.S.C. § 103(a) over ACNS in view of Kjendal and Diffserv;

FURTHER ORDERED that the trial will be conducted in accordance with the accompanying Scheduling Order.

PETITIONER:

Daniel W. McDonald
Jeffrey D. Blake
Kathleen E. Ott
Christopher C. Davis
MERCHANT & GOULD P.C.
dmcdonald@merchantgould.com
jblake@merchantgould.com
kott@merchantgould.com
cdavis@merchantgould.com

PATENT OWNER:

James Hannah
Jeffrey H. Price
Michael Lee
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com

Bradley C. Wright
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com