


PTAB Oral Argument

December 18, 2019

Cisco Systems, Inc. v.  Centripetal
Petitioner Patent Owner

CASE: IPR2018-01512
PATENT NO.: 9,565,213

Summary of Arguments

Technical Issues

- Petitioner's proposed claim construction is vague, ambiguous, and unsupported
- ACNS does not act on a packet-by-packet basis
- ACNS and Kjendal do not teach a dynamic security policy
- ACNS and Kjendal do not teach routing identified packets to a monitoring device in response to performing the packet transformation function
- References do not teach receiving a dynamic security policy with a rule that includes a DSCP selector as the packet identification criteria

'213 Patent – Claim 1

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;

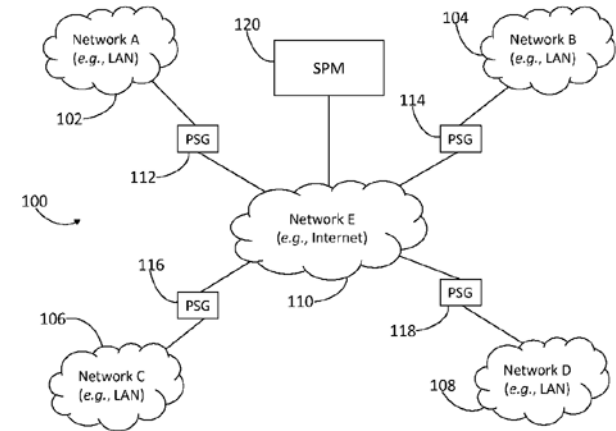


FIG. 1

'213 Patent – Claim 1 (cont)

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

United States Patent
Rogers et al.

(54) METHODS AND SYSTEMS FOR
PROTECTING A SECURED NETWORK

(71) Applicant: Centripetal Networks, Inc., Reston,
VA (US)

(72) Inventors: Steven Rogers, Leesburg, VA (US);
Sean Morris, Falls Church, VA (US)

(10) Patent No.: US 9,565,213 B2
(45) Date of Patent: Feb. 7, 2017

References Cited

U.S. PATENT DOCUMENTS

6,098,173 A
6,226,173 A

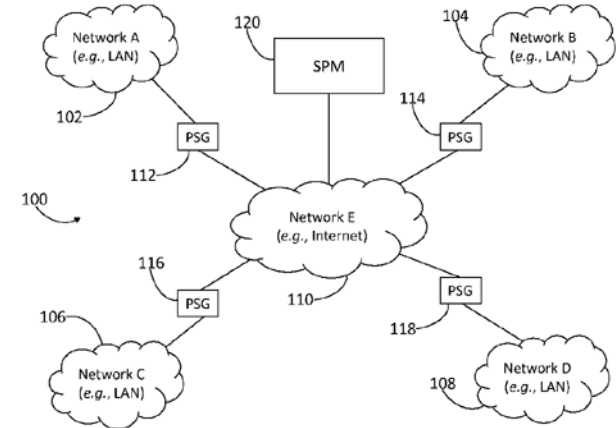


FIG. 1

16 Claims, 13 Drawing Sheets

'213 Patent – Claim 1 (cont)

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.

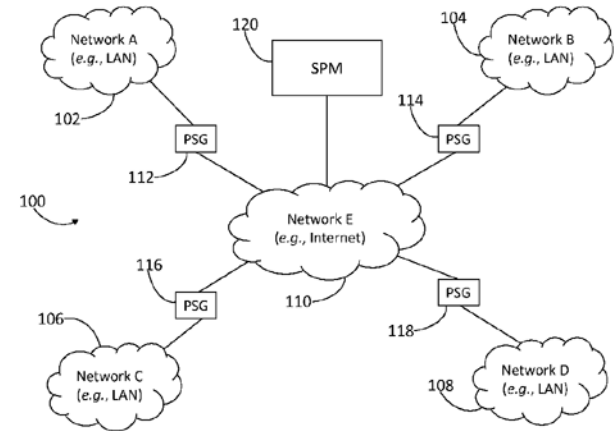


FIG. 1

Claim Construction – Terms to Construe

- “packet”
- “packet-by-packet”
- “dynamic security policy”
- “rule” / “rules”
- “security policy management server”
- “packet security gateway”
- “packet transformation function”
- “monitoring device”

ACNS does not act on a packet-by-packet basis

Representative Claim 1:

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;

ACNS does not act on a packet-by-packet basis

Representative Claim 1 (cont.):

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

ACNS does not act on a packet-by-packet basis

Representative Claim 1 (cont.):

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

Claim Construction – “packet” / “packet-by-packet”

- “packet” means “a link layer (L2) or network layer (L3) packet.” POR at 9-12
 - Petitioner does not dispute this construction.
- “packet-by-packet” means “you’re working a packet at a time.” Sur-Reply at 1-2.
 - Based on Petitioner’s own expert testimony. (Ex. 2022 at 22:19-23:14) (“looking at one packet then looking at another packet and then looking at a third packet.”)
 - Raised in response to Petitioner’s issues of claim interpretation in its Reply.

ACNS does not act on a packet-by-packet basis

ACNS teaches accepting or rejecting HTTP request methods, which requires reassembling L2 and/or L3 communication flows rather than inspecting individual packets:

Adding or Modifying Additional HTTP Request Methods for the Content Engine

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.

ACNS at 8-23; POR at 24-28.

ACNS does not act on a packet-by-packet basis

ACNS teaches creating records of web transactions, not records of individual packets. Transaction logs include:

Using the Transaction Logs

This chapter explains how to use the transaction logs and contains the following sections:

- [Understanding Transaction Log Formats, page 19-1](#)
- [Transaction Logging and NTLM Authentication, page 19-7](#)
- [Usage Guidelines for Log Files, page 19-8](#)
- [Enabling Transaction Logging with the Content Distribution Manager GUI, page 19-10](#)
- [Using WMT Transaction Logging, page 19-15](#)
- [Using Real-Time Transaction Logging, page 19-19](#)

Transaction logs allow administrators to view the traffic that has passed through the Content Engine.

Typical fields in the transaction log are 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.

ACNS at 19-1; POR at 31-35.

ACNS does not teach the claimed packet security gateway

The Content Engine of ACNS is not the claimed packet security gateway

- Eli Fuchs, former senior engineering manager at Cisco testifies that the ACNS Content Engine is not concerned with packets or security.
- The parties and Institution Decision agree that a “packet security gateway” means “a gateway computer configured to **receive packets** and perform a packet transformation function **on the packets.**”

2 Q. Does the content engine perform any
3 security analysis on the request?
4 MR. EVANS: Objection to form.
5 A. The content engine does not perform any
6 inspection of data within the object, no.
7 Q. To be specific, though, does it perform any
8 security analysis on the request itself?
9 MR. EVANS: Objection to form.
10 A. If the request -- does it -- repeat the
11 question? I'm sorry.
12 MR. PROCTOR: Could you please repeat
13 the question.
14 (Last question read.)
15 A. It does not.
16 Q. Does it look at individual packets within
17 the request?
18 MR. EVANS: Objection to form.
19 A. It does not.

ACNS does not teach the claimed packet security gateway

The Content Engine of ACNS is not the claimed packet security gateway

- Petitioner's expert's testimony contradicts the testimony of Cisco's Senior Engineering Manager.
- Petitioner's expert admits the Content Engine cannot inspect payload of packet for malware. POR at 23-24.

8 Q You said, and I quote, so ACNS will allow you
9 to provide security functions related to -- associated
10 with users or with content in the form of request methods
11 or URLs, but what it doesn't allow is it doesn't allow
12 you to, for example, directly inspect the payloads to see
13 if there is malware in the payload. Do you recall --
14 A Yes.
15 Q -- saying that?
16 Why does -- why do you say ACNS doesn't allow
17 you to, for example, directly inspect the payloads to see
18 if there's malware in the payload?
19 A Because I don't believe ACNS discloses the
20 ability to do searching, for example, over payloads.

Ex. 2020 at 68:8-20

Claim Construction – “dynamic security policy”

“a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets.” POR at 12-16.

- Petitioner’s construction improperly removes patentable weight from the word “dynamic.” POR at 15.
- “[C]laims are interpreted with an eye toward giving effect to all terms in the claim.” *Bicon, Inc. v. Straumann Co.*, 441 F. 3d 945, 950 (Fed. Cir. 2006)
- Portion of the ‘213 Patent cited by the Petitioner supports what a dynamic security policy can **include**, not what it is limited to. Sur-Reply at 4-5.

described herein. As used herein, a dynamic security policy includes any rule, message, instruction, file, data structure, 60 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. Optionally, a dynamic security policy may further specify one or more additional parameters as described 65 herein.

‘213 Patent at 4:48-67

ACNS does not teach receiving a dynamic security policy from a security policy management server

ACNS teaches that an Admin may add to or otherwise modify a policy already existing on a Content Engine:

Adding or Modifying Additional HTTP Request Methods for the Content Engine

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.

ACNS at 8-23

ACNS does not teach receiving a dynamic security policy from a security policy management server

- Adding or modifying a request method involves adding one HTTP request method to a plurality of request methods already configured on the Content Engine. POR at 26.
- ACNS only allows for manually adding a request method, either through a GUI or a command line interface. POR at 26-28.
 - Claimed 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.” POR at 29 (citing '213 Patent at 14:56-59.)

ACNS and Kjendal do not teach routing identified packets to a monitoring device in response to performing the packet transformation function

- Neither ACNS nor Kjendal teach “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.
- Kjendal is directed to mirroring packets that have been identified as meeting a criteria, e.g. have the presence of a selected field. Ex. 1009 at 8:64-9:3.
- Petitioner fails to show that Kjendal routes packets **in response** to an operation being performed on the packets. Sur-Reply at 17.

References do not teach receiving a dynamic security policy with a rule that includes a DSCP selector as the packet identification criteria

- Petitioner asserts ACNS and DiffServ disclose utilizing DSCP data
- BUT 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. POR at 55.

Evidence of Long-felt Need for Dynamic Security Policies

- Recognition of problem/failure with signature behavior based systems (e.g., in Narayanaswamy and Kapoor) to keep up with emerging threats demanded new solutions. POR at 61

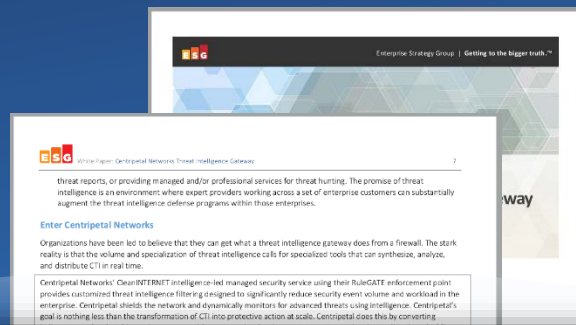


6

Patent Owner Centripetal Networks, Inc. - Ex. 2013, p. 6

Ex. 2013 at 6.

Evidence of Long-felt Need for Dynamic Security Policies (cont.)



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.



Ex. 2006 at 7

Patent Owner Centripetal Networks, Inc. - Ex. 2023
IPR2018-01512 21

Evidence of Industry Praise for Dynamic Security Policies



White Paper: Centripetal Networks Threat Intelligence Gateway

8

The decision rate observed with this much intelligence and this much traffic is in the range of a quintillion (10^{18}) decisions per second.⁷ This is the highest performance network filter that ESG has tested or seen in action to date.

Ex. 2006 at 8

4/26/2019

Top 10 FinTech Companies to Watch | American Banker

Slideshow Top 10 FinTech Companies to Watch

Published November 06 2013, 7:30am EST

More in

Centripetal Networks

Technology: Appliance that provides a "clean internet" by applying millions of rules to fast-moving network traffic.

Why It's One to Watch: The appliance has the potential to detect and deter rapidly changing cybersecurity threats on the fly.

Ex. 2011

Ex. 2011 at 14

Patent Owner Centripetal Networks, Inc. - Ex. 2023
IPR2018-01512 22

Evidence of Industry Praise for Dynamic Security Policies (cont.)

Gartner.

Cool Vendors in Security for Technology and Service Providers, 2017

Published: 4 May 2017 ID: G00321937

Ex. 2007

The QuickThreat Gateway appliance enhances customers' ability to perform more comprehensive threat detection and blocking than traditional network security appliances. The QuickThreat Gateway appliance performs analytics and provides threat alerts by leveraging Centripetal Networks' QuickThreat Manager solution, which correlates and visualizes threats by factors such as severity, reliability and geography. The QuickThreat intelligence service synchronizes and normalizes threat intelligence from more than 40 third parties. The system is **unique because it enables threat feeds, internal or external, to be integrated.**

The QuickThreat Gateway appliance 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. Meanwhile, other multifunction or network security appliances are typically limited to the detection and prevention of only tens of thousands of threat indicators. The QuickThreat system also provides subscriptions to a wide variety of community (such as Financial Services' Information Sharing and Analysis Center [FS-ISAC] and government) and open-source feeds. The system is valuable and cost-effective for enterprises of all sizes. Current customers span

Ex. 2007 at 5