

***Netskope, Inc. v. Fortinet, Inc.***

**IPR2023-00459**

**U.S. Patent No. 10,084,825**

**Patent Owner's Demonstratives**

**Hearing: June 21, 2024**

| Ground                    | Claim(s) challenged          |
|---------------------------|------------------------------|
| 1. Chandra                | 1-5, 12, 15-16, 21-22, 27    |
| 2. Chandra, Buruganahalli | 6-7, 17-18, 23-24, 28-29     |
| 3. Chandra, Kumar         | 10-11                        |
| 4. Chandra, Chandra-2     | 13-14, 19-20, 25-26, 30-31   |
| 5. Keohane                | 1-5, 10-12, 15-16, 21-22, 27 |
| 6. Keohane, Buruganahalli | 6-7, 17-18, 23-24, 28-29     |
| 7. Keohane, Kumar         | 10                           |
| 8. Keohane, Chandra-2     | 13-14, 19-20, 25-26, 30-31   |

| Ground      | Patent Owner's Arguments                                                               | Applies to Claims        |
|-------------|----------------------------------------------------------------------------------------|--------------------------|
| All Grounds | Neither Chandra or Keohane teach a “cooperative security fabric” as properly construed | All Challenged Claims    |
| 1           | Chandra does not disclose “local network policies”                                     | 2, 4, 15                 |
| 1, 5        | Chandra and Keohane do not render obvious flags in a “first packet of a session”       | 12                       |
| 2, 6        | Chandra and Keohane do not render obvious a “next network appliance”                   | 6-7, 17-18, 23-24, 28-29 |
| 6           | Keohane does not render obvious updating or removing flags                             | 6-7, 17-18, 23-24, 28-29 |

# Overview of '825 Patent

# Overview of the '825 Patent: Claim 1

1. A method comprising:  
receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;  
determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;  
when the network traffic is determined to have been transmitted from the second network security appliance:  
determining, by the first network security appliance, one or more network security operations that are executed by the second network security appliance;  
determining, by the first network security appliance, one or more local network security operations that are to be executed by the first network security appliance based on the one or more network security operations that are executed by the second network security appliance, including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance; and  
executing, by the first network security appliance, the one or more local operations on the network traffic.

Ex. 1001 (825 patent) at Claim 1

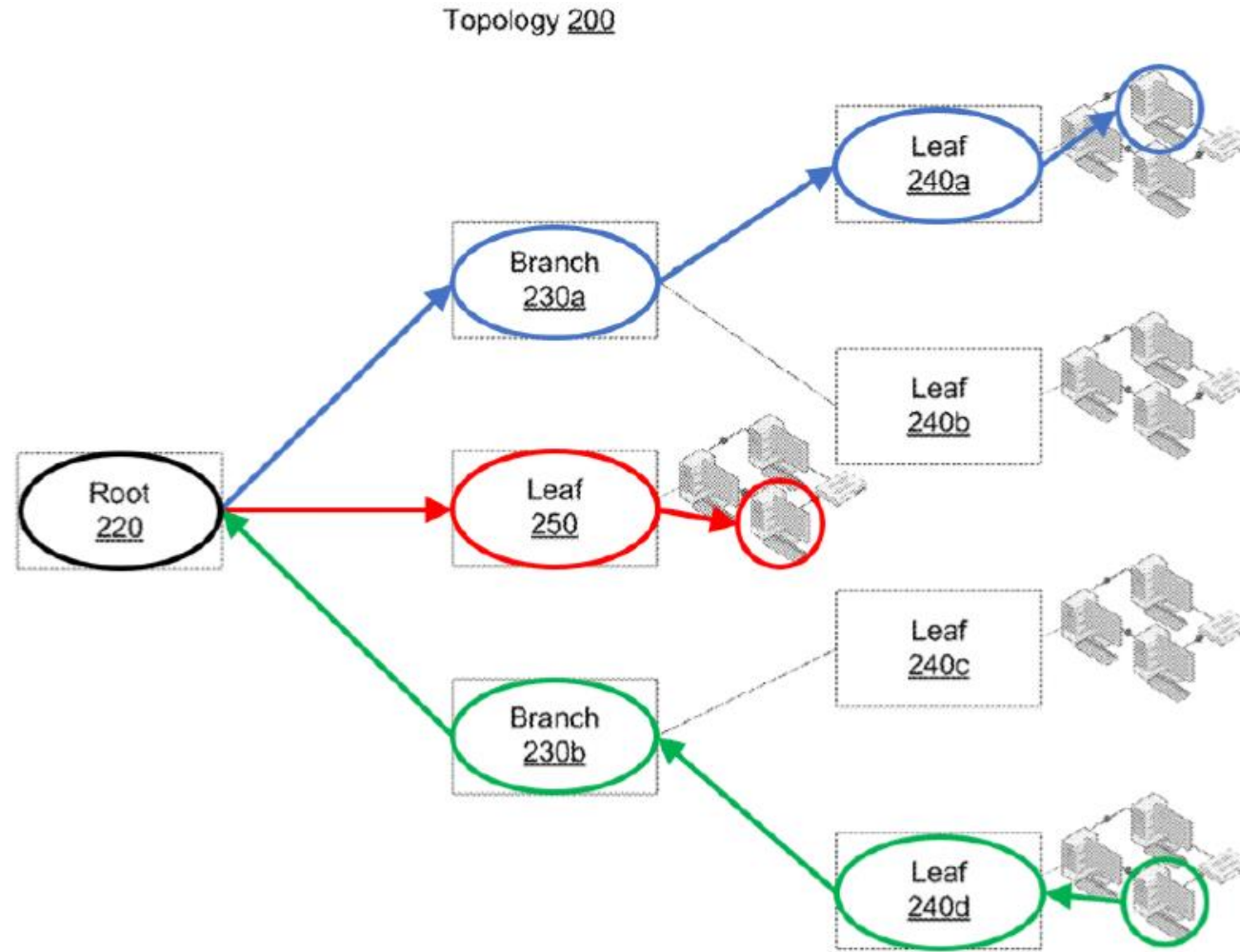
## Overview of the '825 Patent: Problem to be Solved

“In a large network, many network security appliances may be deployed at different locations within the network. Network traffic transmitted to/from the network may go through multiple network security appliances along a path within the network. Usually, a network security appliance may be configured with multiple policies that define security operations to be executed on the incoming network traffic.”

Ex. 1001 (825 Patent) at 1:33-39

# Overview of the '825 Patent: Cooperative Security Fabric

- Inspects incoming / outgoing traffic



Ex. 1001 (825 patent) at Figs. 1, 2 (modified); POR 5

## Overview of the '825 Patent: Cooperative Security Fabric

- Inspects incoming / outgoing traffic

“[D]ownstream network traffic that is transmitted from the Internet 110 to a subnet 141 goes through three network security appliances, i.e. a root, a middle and a subnet network security appliance, while upstream network traffic that is transmitted from subnet 141 to the Internet 110 goes through a subnet, a middle and a root network security appliance.”

Ex. 1001 (825 Patent) at 5:32-38

# Summary of the Prior Art

## Summary of the Prior Art: Chandra (Ex. 1004)

- Figure 2: Internal network traffic

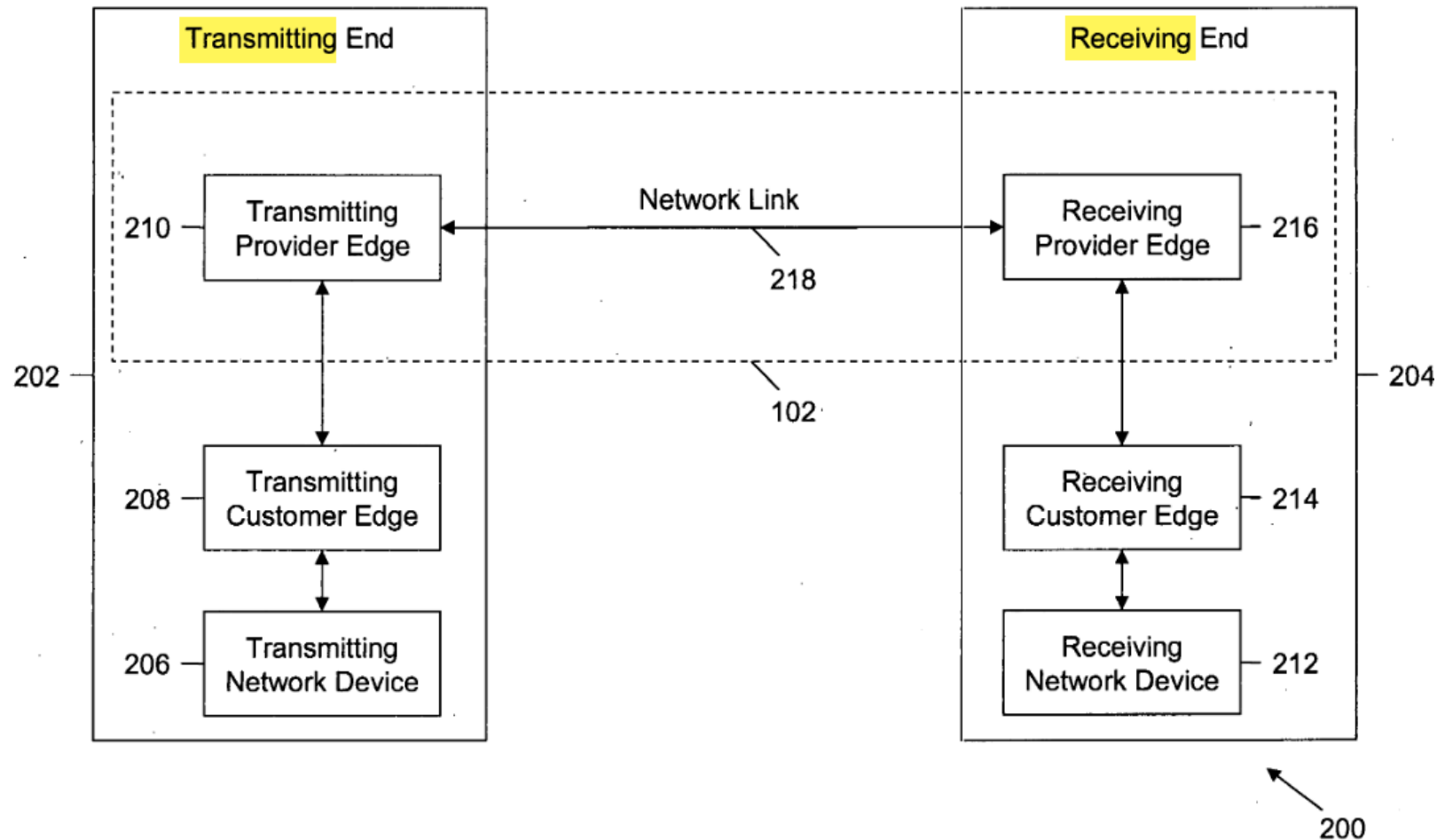
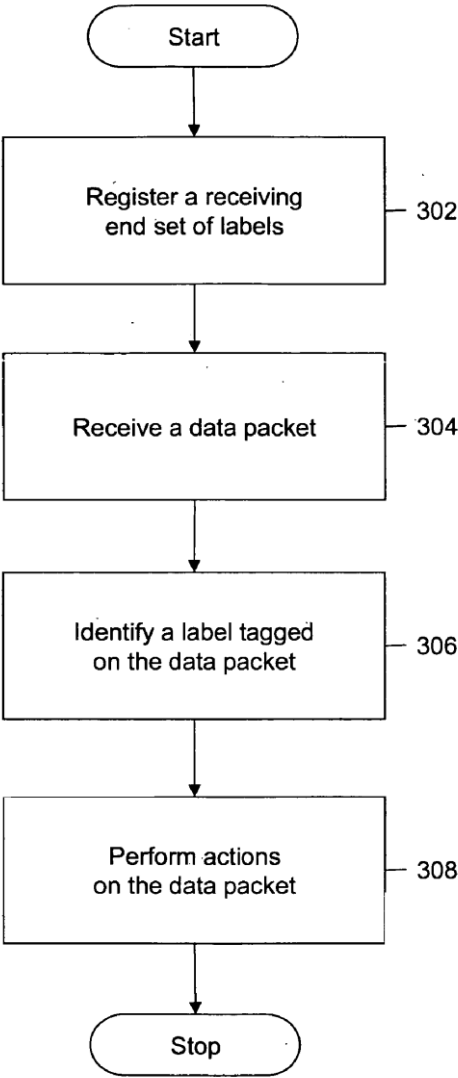


FIG. 2

Ex. 1004 (Chandra) at Fig. 2 (annotated)

# Summary of the Prior Art: Chandra (Ex. 1004)

- Figure 3: Internal network traffic



Labels at **Transmitting** CE

| Label      | Rules         | Receiving CE                |
|------------|---------------|-----------------------------|
| 1256       | Rules A and B | Address of receiving CE 214 |
| 1257       | Rules C and D | Address of receiving CE 214 |
| <untagged> | Rule E        | Address of receiving CE 214 |
| ...        |               |                             |

Labels at **Receiving** CE

| Label      | Rules         | Transmitting CE                |
|------------|---------------|--------------------------------|
| 1256       | Rules A and B | Address of transmitting CE 208 |
| 1257       | Rules C and D | Address of transmitting CE 208 |
| <untagged> | Rule E        | Address of transmitting CE 208 |
| ...        |               |                                |

## Summary of the Prior Art: Chandra (Ex. 1004)

- Internet traffic examined by only **one** CE: no cooperation

“[W]hen receiving CE 214 receives a data packet from the Internet, it performs actions corresponding to rules regarding such data packets.”

Ex. 1004 (Chandra) at ¶53

“[T]he receiving end can identify a data packet from the Internet as insecure, and perform rigorous actions on it.”

Ex. 1004 (Chandra) at ¶77

## Summary of the Prior Art: Keohane (Ex. 1008)

- Two network appliances: Firewall and Mail Gateway
- Only inspects incoming traffic

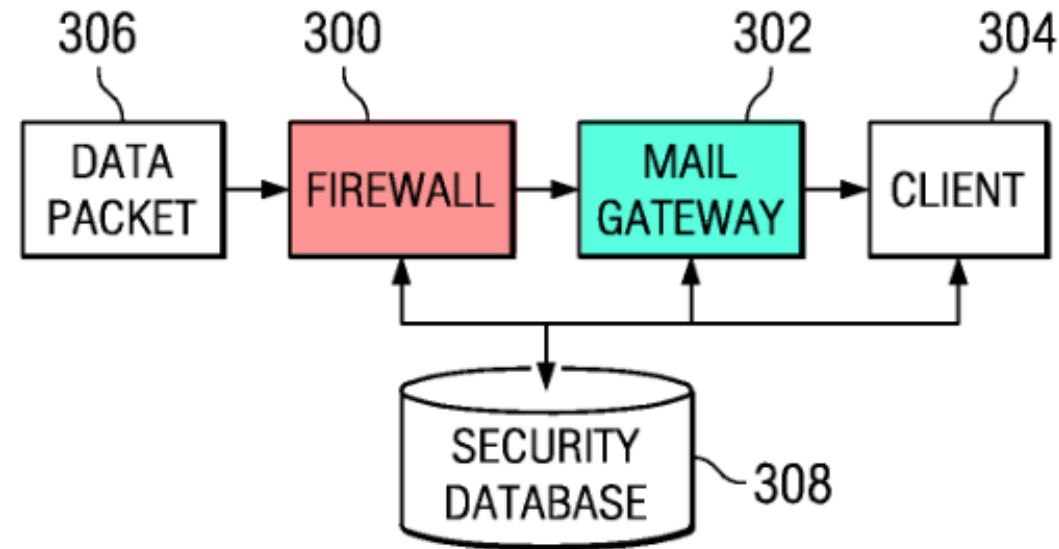
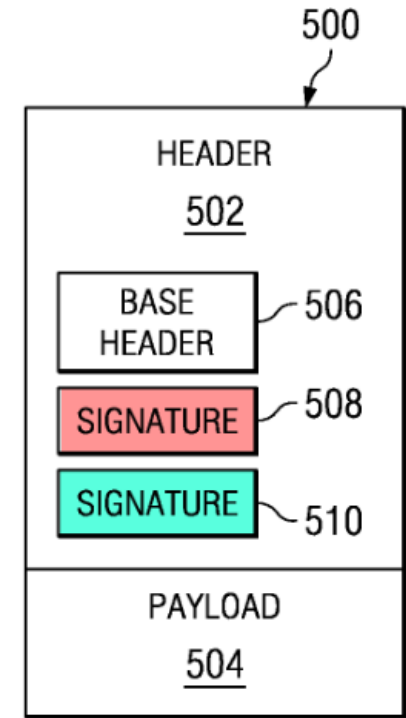
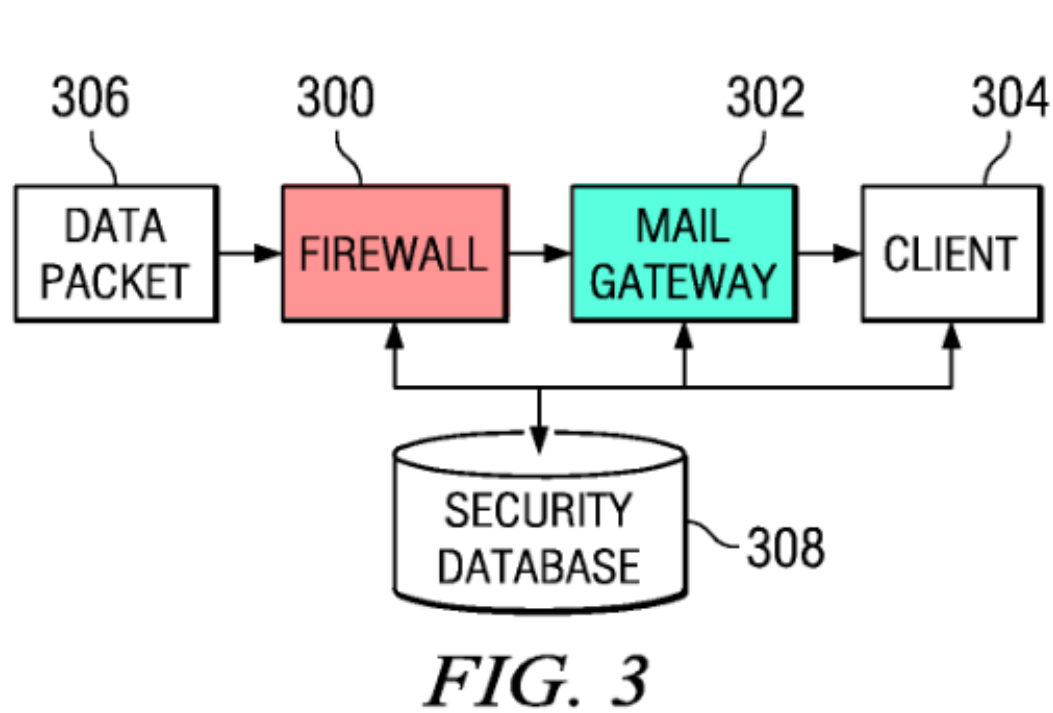


*FIG. 3*

Ex. 1004 (Keohane) at Fig. 3

## Summary of the Prior Art: Keohane (Ex. 1008)

- Each appliance appends a signature to the packet



**The Prior Art does not disclose a “cooperative security fabric (CSF)”  
(All Grounds, All Claims)**

## Summary of arguments for “cooperative security fabric (CSF)”

### Petitioner’s Arguments

Plain meaning of CSF is “devices that form a network topology and work together to coordinate security operations among them”

Only two devices needed to “form a network topology”

Chandra discloses a CSF

Keohane discloses a CSF

### Patent Owner’s Arguments

“CSF” is a term Fortinet created to describe its products

Plain meaning of CSF is “a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths”

Petitioner’s definition overly broad and renders the term superfluous

Chandra does not disclose “cooperat[ing] to inspect incoming and outgoing traffic”

Keohane does not disclose “inspect[ing] ... outgoing traffic” or “multiple interconnected paths”

## Proposed definitions for “cooperative security fabric (CSF)”

### Petitioner’s Definition

“devices that form a network topology and work together to coordinate security operations among them”

### Patent Owner’s Definition

“a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths”

- Points of dispute
  - Whether the CSF must cooperatively inspect “incoming and outgoing traffic” (Chandra, Keohane)
  - Whether the CSF can be two nodes or if instead must have “multiple interconnected paths” (Keohane)

## All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- Undisputed: Fortinet coined the term in 2016, a year before the 825 patent
- Undisputed: “cooperative security fabric” and “CSF” only appear in Fortinet patents, product literature, and marketing literature

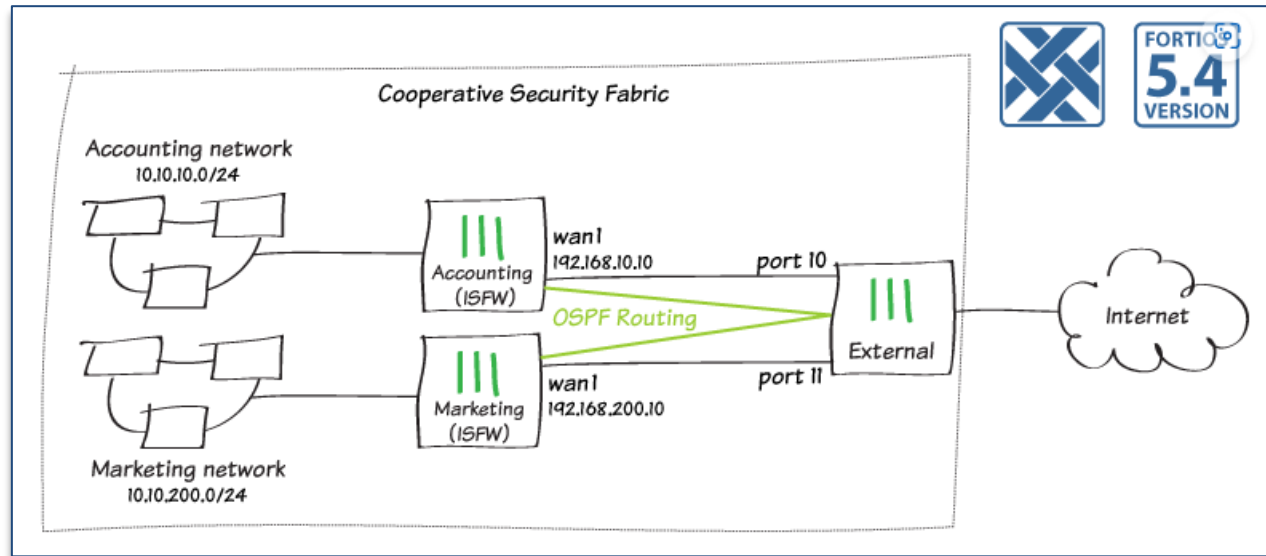
“When performing a search for the phrase ‘cooperative security fabric’ on Google Books, no results were returned. I also performed a search on Google Scholar for any academic papers containing the phrase, and it did not return any results related to network security. When searching for patents or patent applications using Google Patents, the only results that contain ‘cooperative security’ were those assigned to Fortinet, the earliest of which was the ’825 patent. I also used the USPTO and EPO searching sites and likewise only found Fortinet-owned patents and applications.

Finally, I performed a search on Google for the term ‘cooperative security fabric.’ I reviewed the first dozen or so results and each result was either Fortinet documentation or describing a Fortinet product.

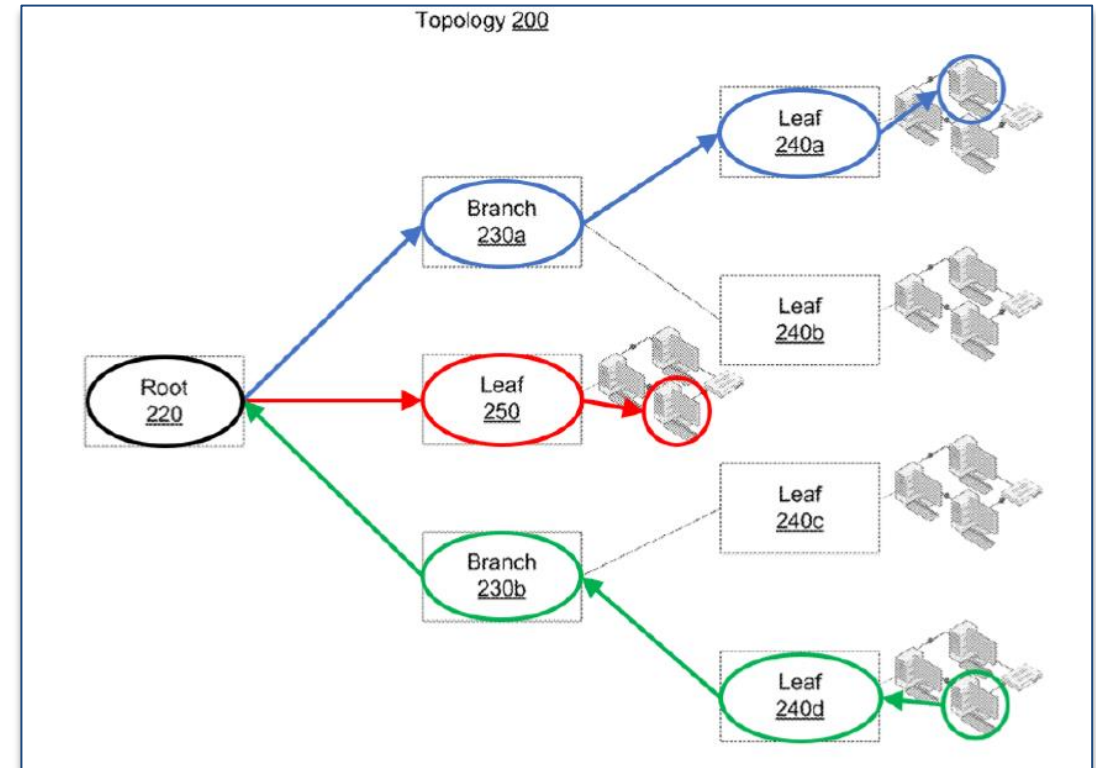
Ex. 2004 (Black Supp. Decl.) at ¶¶68

# All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- Fortinet documents describe CSF as inspecting *incoming/outgoing traffic* and *multiple interconnected paths*



Ex. 2013 at 1



Ex. 1001 (825 Patent) at Figs. 1, 2 (combined, annotated)

# All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- Fortinet documents describe CSF as inspecting *incoming/outgoing traffic* and *multiple interconnected paths*

## 1. Installing a FortiGate in NAT/Route mode

In this recipe, you install the initial FortiGate, which will later be used as the Internet-facing, or upstream, FortiGate in the security fabric.

Because the CSF has not yet been enabled, the FortiView topology dashboards are not yet available.

## 2. Installing internal FortiGates and enabling a security fabric



Watch the video

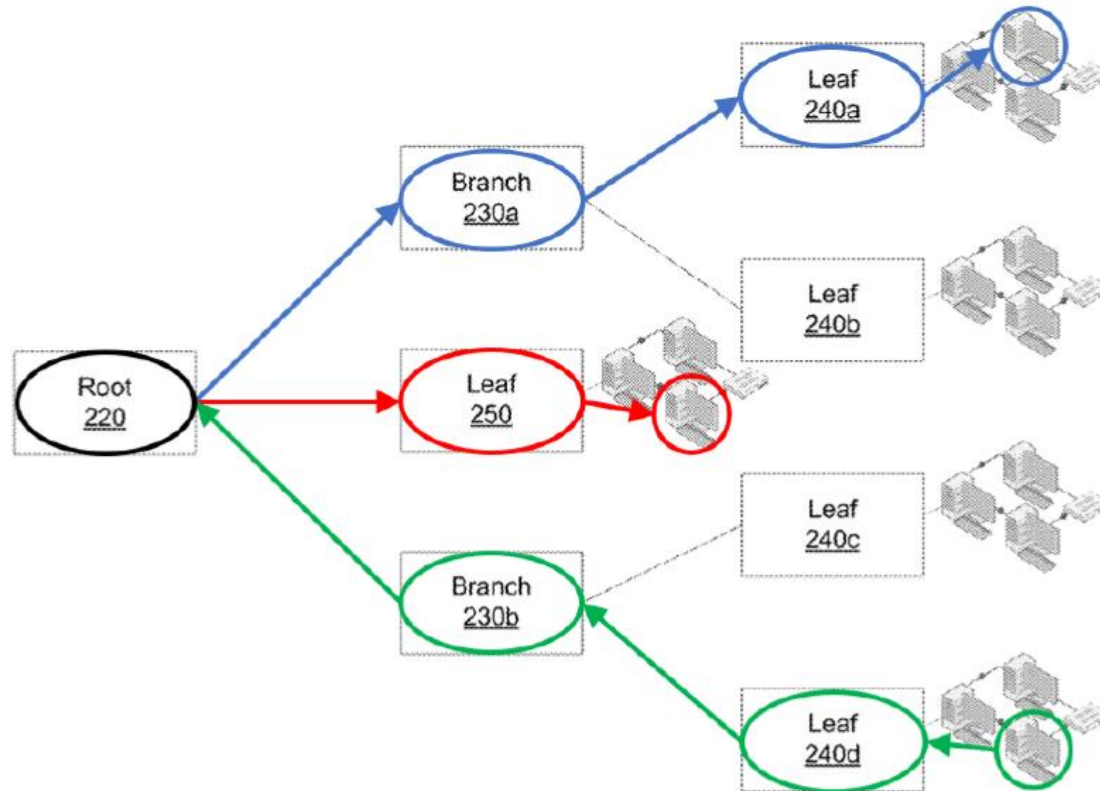
In this recipe, two additional FortiGates are added to the network as an Internal Segmentation Firewalls (ISFWs). Once the FortiGates are installed, a security fabric is set up between them and the external FortiGate which was installed in the network previously.

Ex. 2012 at 2

# All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- All embodiments of the ‘825 Patent inspect *incoming/outgoing traffic* and have *multiple interconnected paths*
- The two-node **red path** is just one of many paths within the CSF

Topology 200



Ex. 1001 (825 patent) at Figs. 1, 2 (modified)

“Topology 200 may have **paths** with no branch nodes, **such as the network path** in which a leaf node 250 is connected to root node 220 directly.”

Ex. 1001 (825 patent) at 18:20

## All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- All embodiments of the ‘825 Patent inspect *incoming/outgoing traffic* and have *multiple interconnected paths*

“In a large network, many network security appliances may be deployed at different locations within the network. Network traffic transmitted to/from the network may go through multiple network security appliances along a path within the network. Usually, a network security appliance may be configured with multiple policies that define security operations to be executed on the incoming network traffic.”

Ex. 1001 (825 Patent) at 1:33-39

“[D]ownstream network traffic that is transmitted from the Internet 110 to a subnet 141 goes through three network security appliances, i.e. a root, a middle and a subnet network security appliance, while upstream network traffic that is transmitted from subnet 141 to the Internet 110 goes through a subnet, a middle and a root network security appliance.”

Ex. 1001 (825 Patent) at 5:32-38

## All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- All embodiments of the ‘825 Patent inspect *incoming/outgoing traffic* and have *multiple interconnected paths*

“And so the CSF has the -- is apparently -- has the **objective** of coordinating security operations on the **network traffic passing through them.**”

Ex. 2005 (Franz Tr.) at 26:4-7

|    |                                                                 |
|----|-----------------------------------------------------------------|
| 10 | Q. Do you agree with the patent office's statement              |
| 11 | that, "The '825 patent describes methods of performing          |
| 12 | security operations on <b>network traffic passing through a</b> |
| 13 | <b>cooperative security fabric, CSF,</b> of network security    |
| 14 | appliances that coordinate their security operations to         |
| 15 | avoid redundant security operations"?                           |
| 16 | A. Yes.                                                         |

Ex. 2005 (Franz Tr.) at 19:10-16

## All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- Petitioner’s expert Dr. Franz confirmed all embodiments of the ‘825 Patent inspect *incoming/outgoing traffic*

|    |                                                     |
|----|-----------------------------------------------------|
| 13 | Q. And you're not aware of other examples in the    |
| 14 | '825 patent that talks about performing security    |
| 15 | operations on traffic between two subnets, are you? |
| 16 | A. In the specification, there's no example like    |
| 17 | that.                                               |

Ex. 2005 (Franz Tr.) at 35:13-17

## All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- The ‘825 Patent is directed to **large, interconnected** networks, not a two-node network

“In a large network, many network security appliances may be deployed at different locations within the network.”

Ex. 1001 (825 Patent) at 1:33-34

“I mean, we have -- we have **more diversity** on the networks. We have **more devices**. We have different networking technologies that coexist. We have devices that move. You know, they are -- they are on the network somewhere. And then they disappear, and they appear somewhere totally different because someone has unplugged a laptop and plugged it in somewhere else. There are -- there are lots of things that, you know, the scale -- everything -- **so many more devices on networks**. So yes, there's more stuff going on.”

Ex. 2017 (Franz Tr.) at 97:20-98:4

## All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- The provisional application’s embodiments inspect *incoming/outgoing traffic* and have *multiple interconnected paths* (i.e. hierarchical interconnections)

“Systems and methods are described for a cooperative security fabric (CSF) protocol that facilitates the dynamic formation of a CSF among multiple network security devices within a private network based on hierarchical interconnections among the network security devices.”

Ex. 2016 (Provisional Application) at ¶13

“In an aspect, the present disclosure relates to a system comprising a cooperative security fabric (CSF) construction module configured to dynamically construct a CSF based on hierarchical interconnections among multiple network security devices deployed within a protected network ... In such an embodiment, a downstream node would not be permitted to query ... a node at the same hierarchical level within the CSF.”

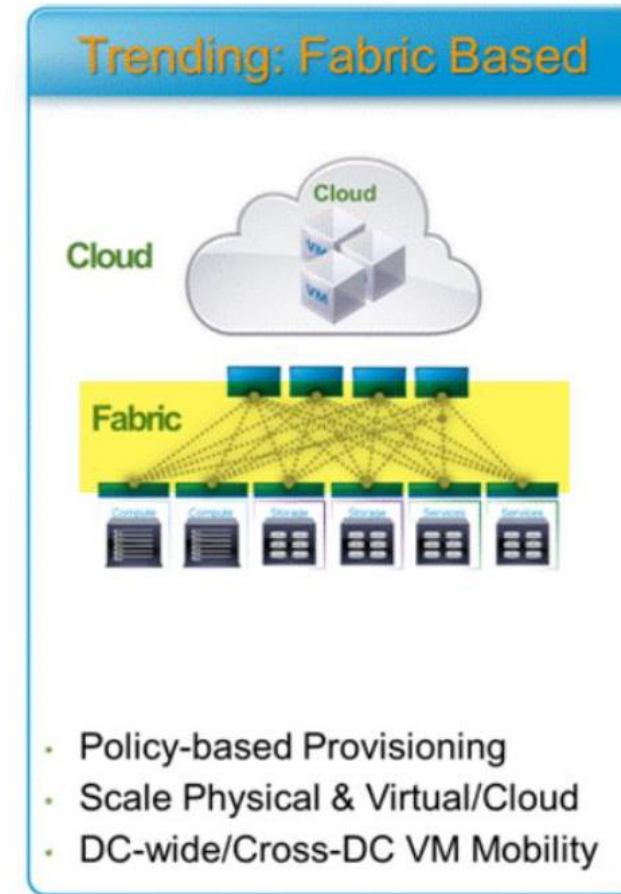
Ex. 2016 (Provisional Application) at ¶18

# All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- Extrinsic evidence: “fabric” requires multiple interconnected paths (multiple threads), not just two nodes (single thread)

**fabric** 1. A descriptive term referring to the physical structure of a switch or network. Much like a piece of cloth, physical/logical communications channels (threads) are interwoven from port-to-port (end-to-end) ... In the Internet, data works its way through a complex, and even unpredictable, interwoven network of networks comprising transmission facilities, packet switches and multiple carriers.

Ex. 2003 (Newton’s Telecom Dictionary)



Ex. 2007 at 167

# All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- Extrinsic evidence: “fabric” requires multiple interconnected paths (multiple threads), not just two nodes (single thread)

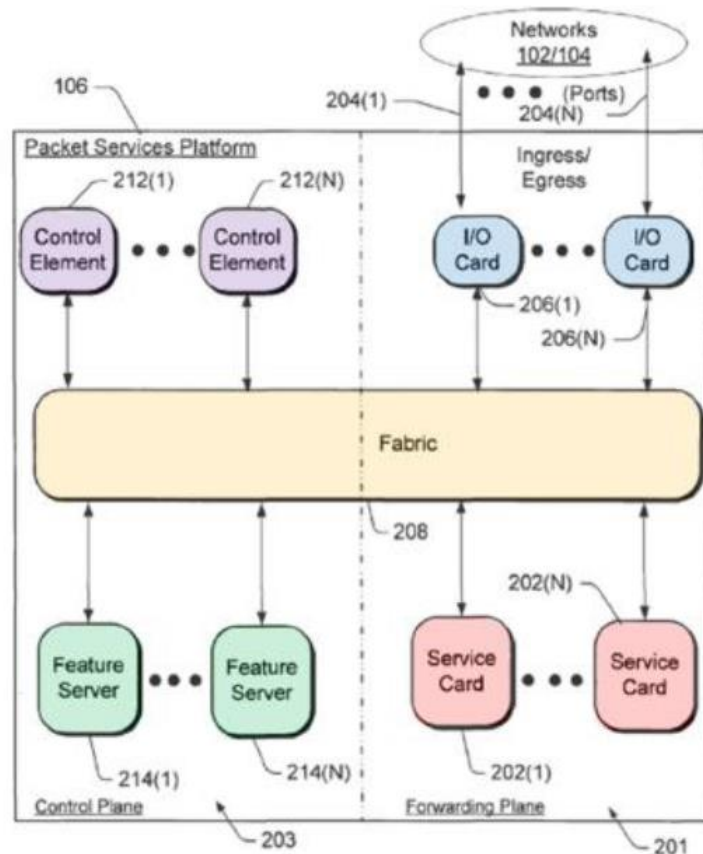


Fig. 2  
(Annotated)

Ex. 2010 at Fig. 2 (annotated by Petitioner)

“I would say in the – POSITA’s term would be: Firewall is part of the so-called security fabric. By ‘fabric,’ I mean **multiple security elements and controls** that one would use or one would want to have. And firewall is part of the – part of the fabric.”

Ex. 2009 (Lee Tr.) at 109:3-7

## All Grounds, All Claims (“CSF”): Patent Owner’s Claim Construction

- Extrinsic evidence: “fabric” requires multiple interconnected paths (multiple threads), not just two nodes (single thread)

Q. You understand the word “fabric” is a reference to clothing fabric; right?

A. So, I mean, I understand that somehow the -- the use of the term in computer science and networking actually sort of may be inspired by the idea that you have **cables weaving**, you know, through buildings and such. So that's probably where the analogy comes from.

Ex. 2005 (Franz Tr.) at 7:24-8:8

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner **ignores** that CSF is a Fortinet-coined term, instead construes each word individually:

### Petitioner’s Definition

“devices that form a network topology and work together to coordinate security operations among them”

“I reviewed the ’825 patent’s claims and found the claim term ‘CSF’ easily understandable from the ordinary usage of its **individual words**. ... Putting these well-understood terms together, a POSITA would have understood the plain meaning of “CSF” as devices that form a network topology and work together to coordinate security operations among them.”

Ex. 1019 (Franz Supp. Decl.) at ¶13

- Petitioner provides **no evidence** on how a POSITA would construe the entire phrase.

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner provides ***no evidence*** on how a POSITA would construe the entire phrase:

Q. Did you search for the term “cooperative security fabric” in any academic papers?

A. I do not think so.

Q. Did you search for the term “cooperative security fabric” in any search engine?

A. I may have done that very early on, but certainly not while writing this -- this rebuttal report.

Q. Did you search for the term “cooperative security fabric” in a library catalog?

A. No.

Q. Did you search for the term “cooperative security fabric” in Google Books?

A. I do not believe it was necessary to do that.

Q. So in preparing this supplemental declaration, you did not search for the term “cooperative security fabric” anywhere; correct?

A. For the -- for the preparation of this rebuttal report, I do not believe so.

Ex. 2017 (Franz Tr.) at 115:21-116:20

Surreply 2

# All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner’s definition renders the term “CSF” and “fabric” superfluous

## Petitioner’s Definition

“[as few as two] devices that form a network topology and work together to coordinate security operations among them”

determining, by the first network security appliance, one or more local network security operations that are to be executed by the first network security appliance based on the one or more network security operations that are executed by the second network security appliance, including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance; and

Ex. 1001 (825 Patent) at cl. 1

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner’s definition renders the term “CSF” and “fabric” superfluous



“It is *highly disfavored* to construe terms in a way that renders them void, meaningless, or superfluous.”

*Wasica Fin. GmbH v. Cont'l Automotive Systems, Inc.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017); Surreply 9

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Dr. Franz’s opinion on “fabric”:

Q. Well, I’m asking: Do you have an understanding of the term “fabric” in the context of distributed computing?

A. I would not want to answer that under oath without doing some additional research, you know, to make sure that my understanding is totally consistent with – yeah.

Ex. 2005 (Franz Tr.) at 16:1-7

# All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner: Patent Owner’s definition—
  - precludes inspection of internal traffic
  - limited to Internet traffic
- Patent Owner’s construction does not **exclude** inspection of internal traffic (“comprising”) nor is it limited to Internet traffic

## Patent Owner’s Definition

“a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths”

“Petitioner is incorrect [that] a CSF need only process purely internal network traffic (such as VPN traffic or subnetwork-to-network traffic).”

POR 19

“I just want to be clear that when I say ‘incoming’ ... I’m talking about traffic **external from the network** arriving to the network.”

Ex. 1018 (Black Tr.) at 32:1-9

Surreply 7-8

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner: Patent Owner’s definition—
  - requires three appliances
  - requires paths that do not share a starting/ending point
  - requires more than one “thread” within the fabric
- These are not “hidden limitations,” they are expressly part of Patent Owner’s definition:

### Patent Owner’s Definition

“a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths”

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner: 825 Patent has internal-only cooperation with VPN traffic
- The 825 Patent does not disclose that VPN traffic is inspected by the CSF
- The 825 Patent says the VPN is a subnetwork, and Dr. Franz admitted the 825 patent does not disclose inspecting traffic between subnetworks

“In this example, a [VPN] subnet 151 and a subnet network security appliance 150 are connected to private network 120 through the Internet 110 via VPN.”

Ex. 1001 (825 Patent) at 4:65-67

|    |                                                     |
|----|-----------------------------------------------------|
| 13 | Q. And you're not aware of other examples in the    |
| 14 | '825 patent that talks about performing security    |
| 15 | operations on traffic between two subnets, are you? |
| 16 | A. In the specification, there's no example like    |
| 17 | that.                                               |

Ex. 2005 (Franz Tr.) at 35:13-17

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner: provisional application discloses one-node CSF
- Petitioner relies on a quote where the CSF is “*initially*” set up
- No dispute that one node is not a CSF

“According to one embodiment CSF 100 can be dynamically constructed and maintained in a recursive way based on the downstream-upstream relationships defined by the **hierarchical interconnection** of the network security devices within the private network. For example, NSD 1 102, having no parent, may ***initially* represent a CSF** containing only one member. The other NSDs 104a-i, having one or more upstream NSDs, may join the CSF to which its parent belongs as described further below. **Once CSF 100 stabilizes**, the root node, i.e., NSD 1 102, **has full information regarding CSF 100**.”

Ex. 2016 (Provisional Application) at ¶26

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner: the provisional application discloses a single-path CSF (“tunneling”)
- Tunneling refers to creating a tunnel on a single path **of a multi-path CSF**
- No dispute “hierarchical interconnections” require multiple paths

“Collectively, CSF construction module 202 of each of the NSDs within a private network dynamically constructs a CSF based on the **hierarchical interconnections** among them by determining its relative position as a root, intermediate or leaf node. ...

Tunnel based communication module 204 **establishes** tunnels between NSD 200 and its parent, if any, and each of its children, if any.”

Ex. 2016 (Provisional Application) at ¶¶40-41

## All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner: claim 1 of the provisional application discloses CSF with a single path
- Claim 1 requires “hierarchical interconnections”
- No dispute that “hierarchical interconnections” requires multiple interconnected paths

1. A method comprising:  
dynamically constructing a cooperative security fabric (CSF) of a plurality of network security devices deployed within a protected network in a form of a tree, having a plurality of nodes, including a root node, one or more intermediate nodes and one or more leaf nodes, based on hierarchical interconnections among the plurality of network security devices by determining a relative upstream or downstream relationship among each network security device of the plurality of network security devices, wherein each node of a plurality of nodes within the CSF represents a network security device of the plurality of network security devices and each node of the CSF, except the root node and the one or more leaf nodes, includes both a parent node and one or more child nodes;

Ex. 2016 (Provisional Application) at cl. 1

# All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

- Petitioner: Fortinet document description of OSPF implies that the CSF need only inspect internal traffic.
- OSPF is a separate function that can be enabled **before** enabling a CSF

## 4. Configuring OSPF routing between the FortiGates

## 5. Enabling the Cooperative Security Fabric

On the External FortiGate,  
go to **System >**

**Cooperative Security  
Fabric. Enable**

**Cooperative Security  
Fabric (CSF) and set a  
Group name and Group  
password.**

☒ **Cooperative Security Fabric (CSF)**

Group name

Office-CSF

Group password

••••••••

Connect to upstream FortiGate ☐

Ex. 2013 at 5, 7-8

Surreply 11-12

# All Grounds, All Claims (“CSF”): Petitioner’s Claim Construction Arguments

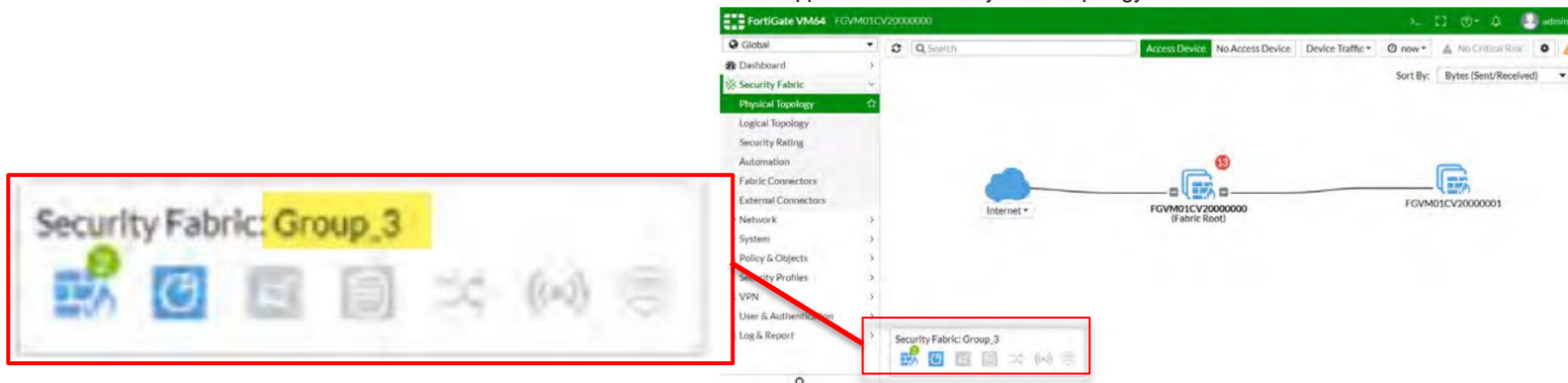
- Petitioner: Fortinet document shows a two-node CSF
- Document is about pre-authorizing a Fortigate to an “**existing fabric**”
- Document indicates the fabric has **additional groups of nodes**

## To pre-authorize a FortiGate:

1. On the root FortiGate, go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
2. In the *Pre-authorized devices*, click *Edit*. The *Pre-Authorized Devices* window opens.
3. Add a new FortiGate to the list using the downstream device's serial number.



4. On the downstream FortiGate, go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
5. For *Status*, click *Enable*.
6. Set *Security Fabric role* to *Join Existing Fabric*.
7. Enter the IP address of the root FortiGate in the *Upstream FortiGate IP* field.
8. Click *OK*.
9. On the root FortiGate, go to *Security Fabric > Physical Topology* and verify that the downstream FortiGate that you added appears in the Security Fabric topology.



## Summary of arguments that Chandra does not disclose “CSF”

### Petitioner’s Arguments

Chandra’s Transmitting CE and Receiving CE form a “CSF”

### Patent Owner’s Arguments

Chandra’s Transmitting CE and Receiving CE is not a CSF because they only inspect internal traffic, not incoming/outgoing traffic

Chandra inspect Internet traffic only through a *single* CE, without any cooperation

# All Grounds, All Claims (“CSF”): Chandra does not disclose a CSF

- Chandra’s CEs cooperate only for *internal traffic within the same network*

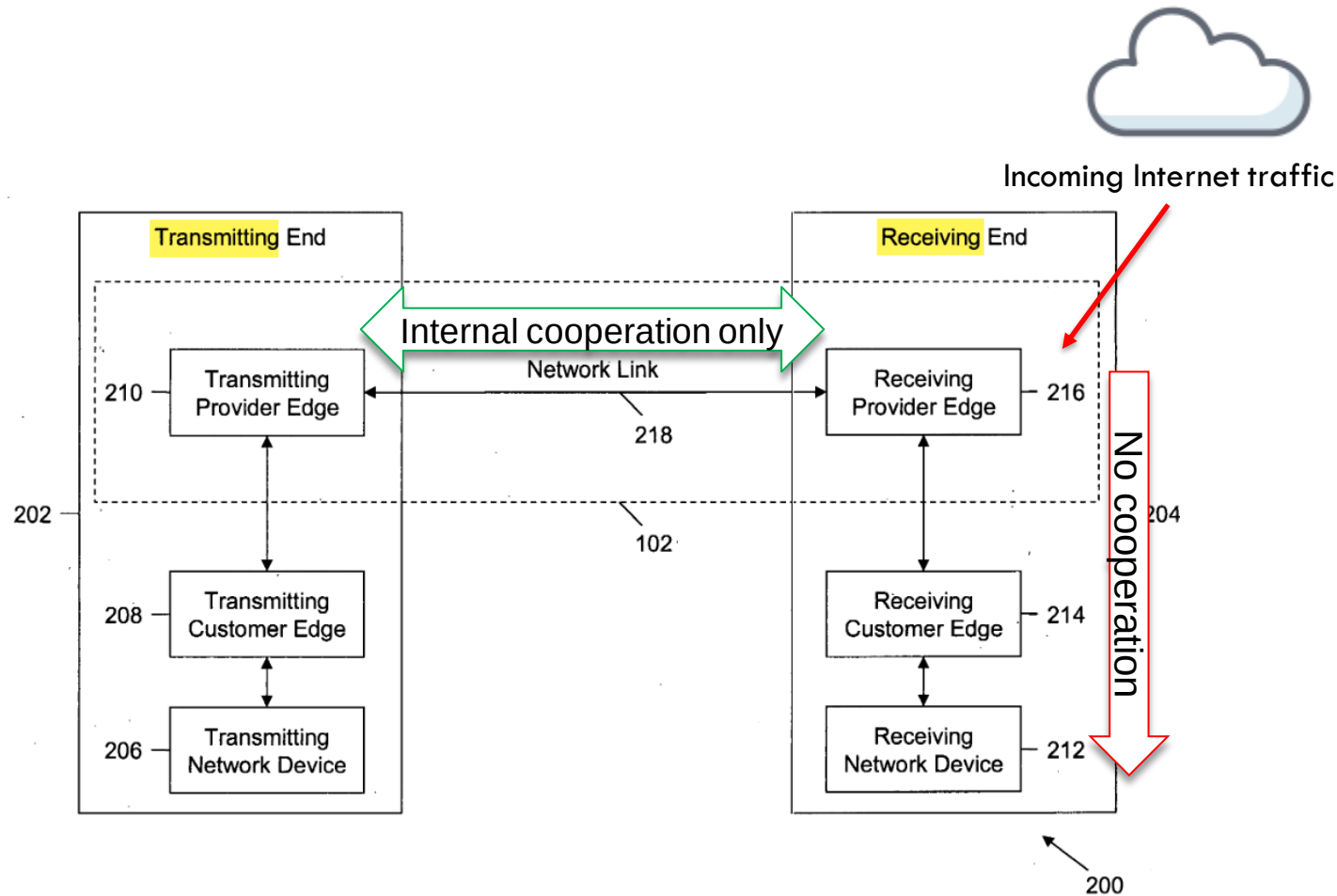


FIG. 2

Ex. 1004 (Chandra) at Fig. 2 (annotated)

“[T]ransmitting end 202 and receiving end 204 can be any identifiable part or region of **network 102**.”

Ex. 1004 (Chandra) at ¶29

“[B]oth the transmitting end and the receiving end are connected to the **same network 102**.”

Ex. 2005 (Franz Tr.) at 41:13-16

## All Grounds, All Claims (“CSF”): Chandra does not disclose a CSF

- Petitioner: Chandra inspects Internet traffic
- Chandra inspects incoming Internet traffic with **only** the “receiving end,” no **cooperation** when inspecting Internet traffic

“[T]he **receiving end** can identify a data packet from the Internet as insecure, and perform rigorous actions on it.”

Ex. 1004 (Chandra) at ¶77

“[C]ooperation require[s] **more than one [device]**, it] requires at least two to cooperate.”

Ex. 2017 (Franz Tr.) at 117:12-14

# All Grounds, All Claims (“CSF”): Keohane does not disclose a CSF

## Summary of arguments that Keohane does not disclose “CSF”

### Petitioner’s Arguments

Keohane’s Firewall and Mail Gateway form a “CSF”

### Patent Owner’s Arguments

Keohane’s Firewall and Mail Gateway are not a CSF because they do not inspect outgoing traffic

Keohane’s Firewall and Mail Gateway are not a CSF because they only form a single path, not “multiple interconnected paths”

## All Grounds, All Claims (“CSF”): Keohane does not disclose a CSF

- Keohane does not disclose a CSF’s inspection of *outgoing* traffic:

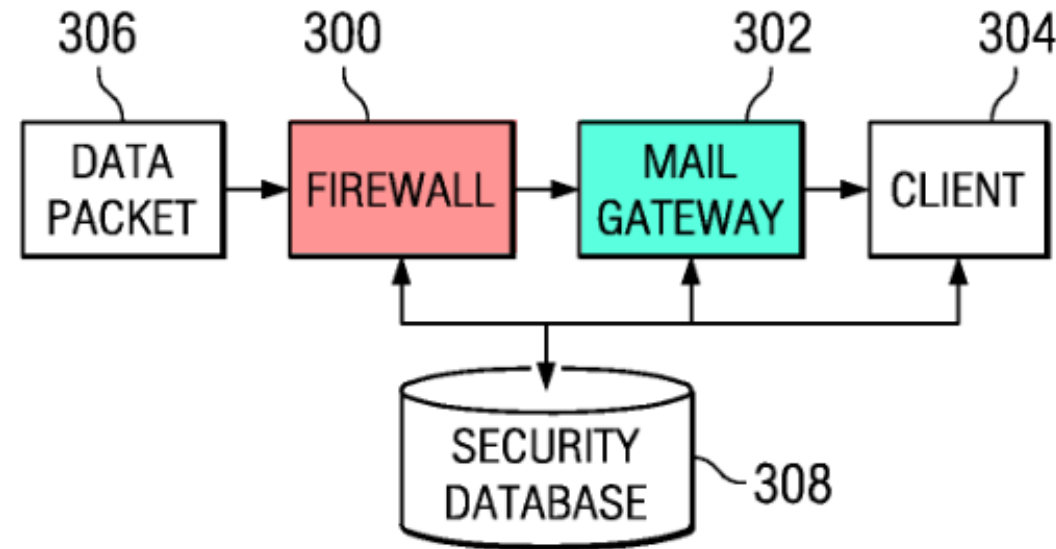


*FIG. 3*

Ex. 1004 (Keohane) at Fig. 3

## All Grounds, All Claims (“CSF”): Keohane does not disclose a CSF

- Keohane does not disclose a CSF’s inspection of **outgoing** traffic.
- Keohane’s “security actions” are only performed on **incoming** traffic:

“[A]n action taken on a data packet in an effort to prevent the introduction [into the network] of malware.”

Ex. 1004 (Keohane) at ¶33

- Keohane’s “security actions” determine if the packet came from a trusted source, *i.e.* incoming traffic

“[The s]ecurity action may be the determination of whether the data packet is from a trusted source.”

“[Keohane’s] security appliances ... trust each other.”

Ex. 1019 (Franz Supp. Decl.) at ¶72

## All Grounds, All Claims (“CSF”): Keohane does not disclose a CSF

- Petitioner: Keohane discloses **multiple interconnected paths** because mail gateway 302 receives incoming traffic (“signatures”)
- Keohane does not disclose that mail gateway 302 receives incoming traffic
- Keohane’s signatures are **internal** and indicate a security action has been performed

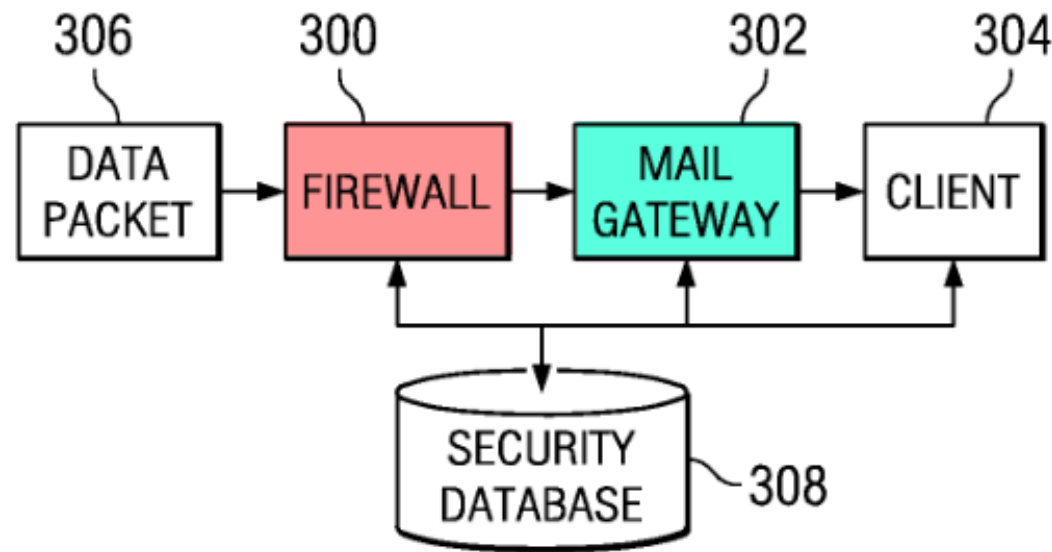


*FIG. 3*

Ex. 1004 (Keohane) at Fig. 3

“[W]ho knows how the network is architected. Again, the flowchart is illustrative to the **specific method** that is described in [Keohane] ... [W]e **don’t know what else is happening** in this network.”

Ex. 2005 (Franz Tr.) at 59:1-12

“The signature indicates that a previous security action has been performed on the data packet.”

Ex. 1004 (Keohane) at Abstract

**Chandra does not disclose “local network policies”  
(Ground 1, Claims 2, 4, 15)**

Summary of arguments for Chandra’s lack of “local network policies”

| Petitioner’s Arguments                                                                        |
|-----------------------------------------------------------------------------------------------|
| Petition: Chandra’s Receiving and Transmitting CEs have locally-stored policies               |
| Reply: Chandra’s Receiving and Transmitting CEs local policies are the “executing algorithms” |

| Patent Owner’s Arguments                                                                |
|-----------------------------------------------------------------------------------------|
| All CE’s get the same policies, they are therefore global policies, not local policies. |
| The executing algorithms cannot be the policy under the claim language.                 |
| The CE’s have the same executing algorithms and same ruleset, so they are global.       |

Ground 1, Claims 2, 4, 15(“local network policies”): Chandra

- Chandra’s CE label rules are not “local” because they are the same for every CE, *i.e.* global

Labels at Transmitting CE

| Label      | Rules         | Receiving CE                |
|------------|---------------|-----------------------------|
| 1256       | Rules A and B | Address of receiving CE 214 |
| 1257       | Rules C and D | Address of receiving CE 214 |
| <untagged> | Rule E        | Address of receiving CE 214 |
| ...        |               |                             |

“[P]olicies [are] uniform among all the VPN sites within a VPN.”

Ex. 1004 (Chandra) at ¶¶6

Labels at Receiving CE

| Label      | Rules         | Transmitting CE                |
|------------|---------------|--------------------------------|
| 1256       | Rules A and B | Address of transmitting CE 208 |
| 1257       | Rules C and D | Address of transmitting CE 208 |
| <untagged> | Rule E        | Address of transmitting CE 208 |
| ...        |               |                                |

Ex. 1004 (Chandra) at ¶¶51-53

## Ground 1, Claims 2, 4, 15(“local network policies”): Chandra

- Petitioner on Reply : “network policies” are “executing algorithms”
  - Inconsistent with language of claims
  - Chandra’s “executing algorithms” and rules are the same and global

### Claim 4 recites “executing ... operations specified by ... local policies”

4. The method of claim 1, further comprising when the network traffic is not transmitted from the second network security appliance, **executing**, by the first network security appliance, one or more local network security **operations specified by one or more local policies**.

Ex. 1001 (825 Patent) at cl. 4

“[R]eceiving CE 214 refers to the receiving CE table, and determines that actions corresponding to rules A and B have been performed on the data packet by transmitting CE 208. Therefore, receiving CE 214 can obviate these redundant actions.”

Ex. 1004 (Chandra) at ¶53

**Chandra and Keohane do not render obvious flags in a “first packet of a session”**

**(Grounds 1 and 5, Claim 12)**

### Summary of arguments for “first packet of a session”

#### Petitioner’s Arguments

Obvious to include flags in “first packet of a session” because it would be “sufficient” to do so

#### Patent Owner’s Arguments

“Sufficient to do so” is not a motivation to combine.

Chandra discloses that authentication and exchange of labels must be performed first.

## Grounds 1, 5, Claim 12 (“first packet of a session”)

- Claim 12 recites carrying a flag in “a first packet of a session”

**12.** The method of claim 1, wherein the one or more packets in which the flag is carried comprises a first packet of a session.

Ex. 1001 (852 Patent) at cls. 6-7

## Grounds 1, 5, Claim 12 (“first packet of a session”): Chandra and Keohane

- Petition provided no rationale beyond that it “would be sufficient”
- Petitioner’s expert parrots the language

“[I]ncluding the flag(s) in the first packet would be sufficient since all of the packets in a session travel back and forth between these two end points.”

Pet. at 44

“[I]ncluding the flag(s) in the first packet would be sufficient since all of the packets in a session travel back and forth between these two end points.”

Ex. 1002 (Franz Decl.) at 101

## Grounds 1, 5, Claim 12 (“first packet of a session”): Chandra

- Chandra discloses handshakes for the session before flags are sent
- Petitioner: authentication and label exchange involves a different session.
  - No evidence to support Petitioner’s argument

“Once transmitting CE 208 and receiving CE 214 **authenticate** each other, they can **exchange the CE labels** to be used for tagging the data packets.”

Ex. 1004 (Chandra) at ¶34

“Transmitting CE and receiving CE coordinate which actions to perform on the network traffic by using labels that are used to tag the data packets. Prior to that, the transmitting CE and receiving CE will first ‘authenticate each other’ and exchange the ‘CE labels that can be used for tagging the data packets.’”

Ex. 2004 (Black Supp. Tr.) at ¶37

**Chandra and Keohane do not render obvious a “next network appliance”**

**(Grounds 2 and 6, Claims 6-7, 17-18, 23-24, 28-29)**

Summary of arguments for “next network appliance”

| Petitioner’s Arguments                                                            |
|-----------------------------------------------------------------------------------|
| Chandra discloses a “next network appliance” in the form of the receiving device  |
| Chandra’s networks could be chained together to obtain a “next network appliance” |
| Keohane discloses a “next network appliance” in the form of the receiving device  |

| Patent Owner’s Arguments                                                             |
|--------------------------------------------------------------------------------------|
| A receiving device is not a “network appliance”                                      |
| Petitioner’s combination of Chandra’s networks lack motivation and would be insecure |

## Grounds 2, 6, Claims 6-7, etc. (“next network appliance”)

- Claims 6-7, 17-18, 23-24, 28-29 recite transmitting the network packet to a “next network appliance”

6. The method of claim 1, further comprising:  
updating, by the first network security appliance, the flag  
to indicate the network security operations executed by  
the first network security appliance; and  
transmitting, by the first network security network appliance, the network traffic with the updated flag to a next network appliance participating in the CSF.

7. The method of claim 1, further comprising:  
removing, by the first network security appliance, the flag  
from the network traffic; and  
transmitting, by the first network security network appliance, the network traffic without the flag to a next network appliance.

Ex. 1001 (852 Patent) at cls. 6-7

## Grounds 2, 6, Claims 6-7, etc. (“next network appliance”): Chandra

- Chandra only discloses **two** network appliances: receiving CE and transmitting CE
  - No other network appliances

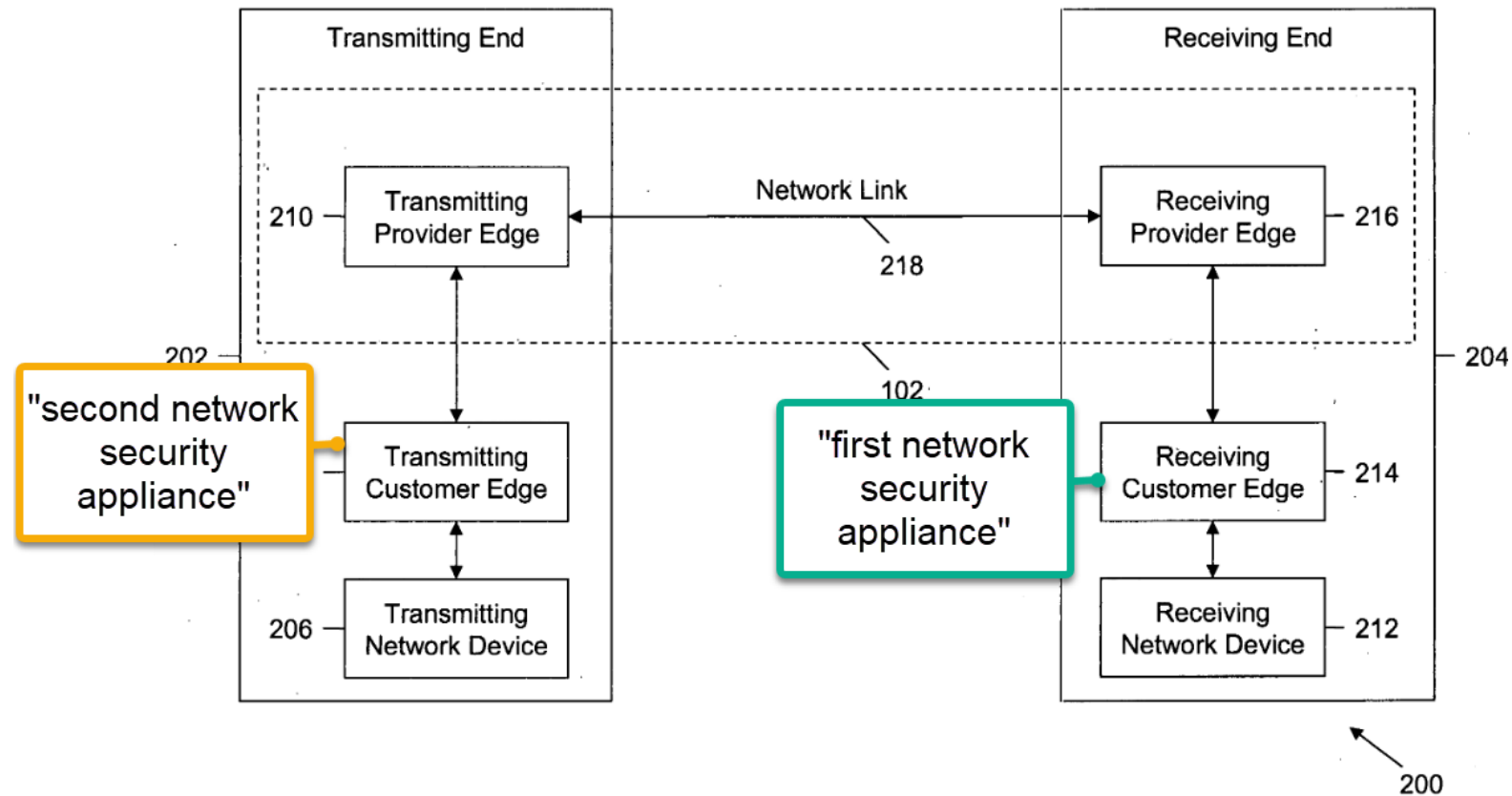
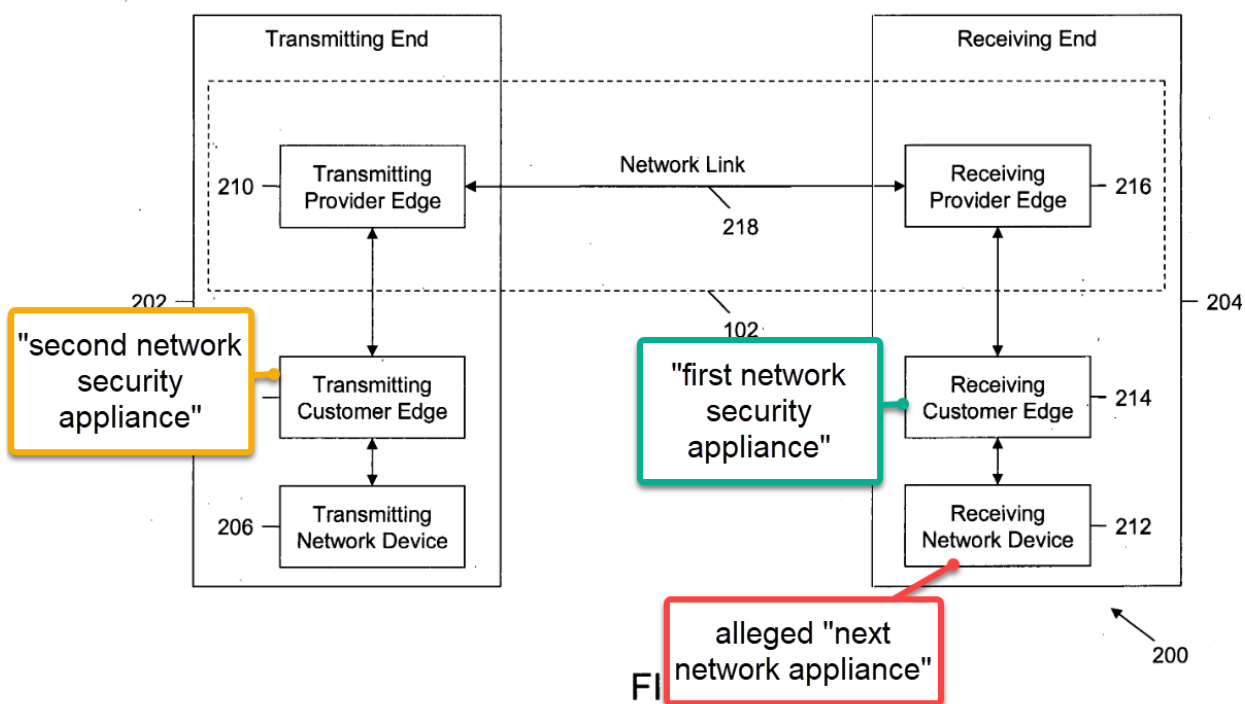


FIG. 2

Ex. 1004 (Chandra) at Fig. 2 (annotated)

## Grounds 2, 6, Claims 6-7, etc. (“next network appliance”): Chandra

- Petitioner argues Receiving Network Device 212 is a “network appliance”
  - Not a network appliance, it is a client device



Ex. 1004 (Chandra) at Fig. 2 (annotated)

“Network devices 104 may be, for example, personal computers, servers, mobile phones, etc.”

Ex. 1004 (Chandra) at ¶21

“The phrase ‘network appliance’ generally refers to a specialized or dedicated device for use on a network in virtual or physical form. ... Examples of functionality include ... Layer 2/3 routing, content inspection, content filtering, firewall ...”

Ex. 1001 (852 Patent) at 4:1-11

“[A]pppliance[s] [have] the property that they are ... devices with a small operating system that ... requires very little interaction and that does ... a small set of specific tasks, mostly without requiring interaction.”

Ex. 2017 (Franz Tr.) at 102:1-9  
POR 42-47; Surreply 19-22

- No response in Petitioner Reply

## Grounds 2, 6, Claims 6-7, etc. (“next network appliance”): Chandra

- Petitioner: Chandra discloses additional customer edges
- No disclosure in Chandra that receiving customer edge 214 sends data to another customer edge
- Petitioner provides no motivation to have another customer edge be the “next network appliance”

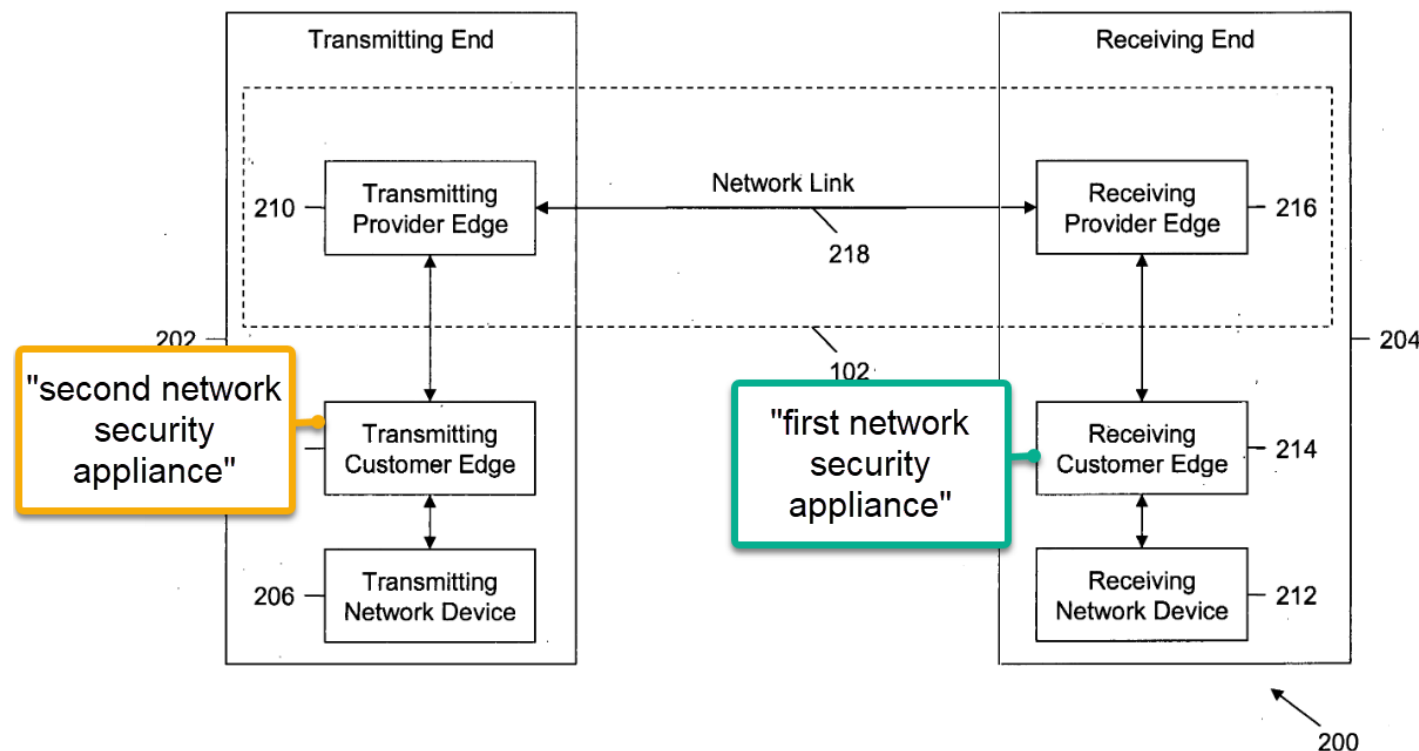


FIG. 2

Ex. 1004 (Chandra) at Fig. 2 (annotated)

## Grounds 2, 6, Claims 6-7, etc. (“next network appliance”): Chandra

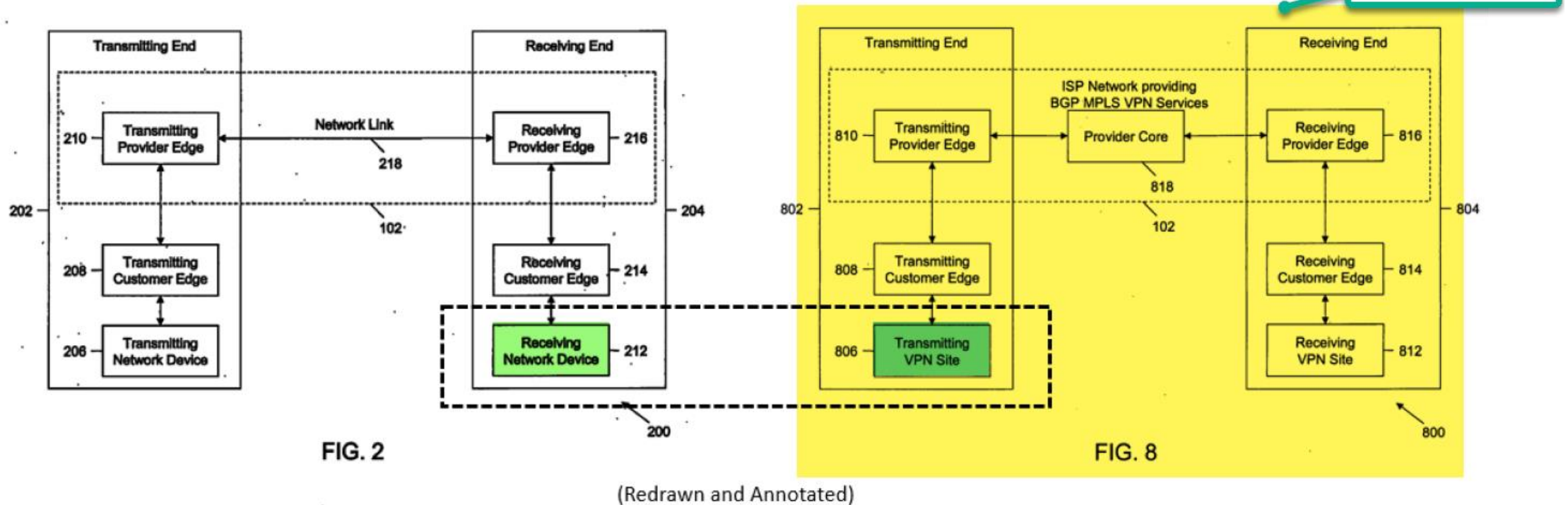
- Petitioner: Buruganahalli renders obvious a “next network appliance”
  - Undisputed: Buruganahalli’s devices are not in a CSF
  - Petition provided no motivation to combine
  - Petitioner Reply abandoned argument

“Buruganahalli only teaches processing packets along a single sequence ... Those devices are thus not part of a ‘fabric.’ ... Petitioner also provides no reason for adding Buruganahalli’s additional network devices to Chandra.”

Ex. 2005 (Black Supp. Decl.) at ¶106

## Grounds 2, 6, Claims 6-7, etc. (“next network appliance”): Chandra

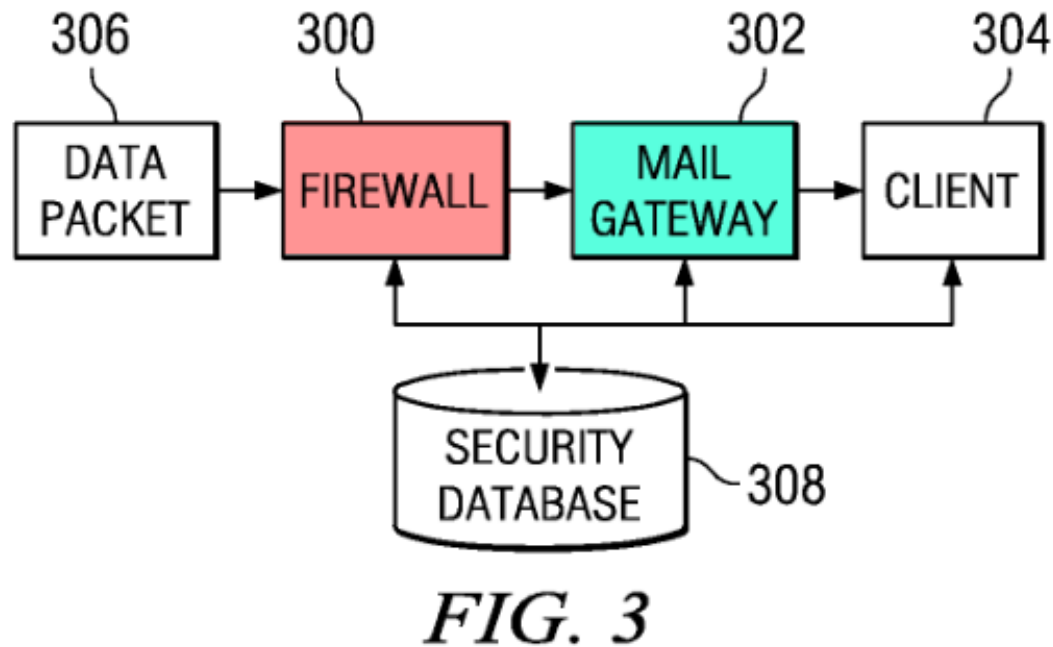
- Petitioner: obvious to modify Chandra to include a “next network appliance”
- Petitioner relies on a contrived, modified figure:



- Petitioner provides no reason why “receiving network device” 212 would transmit data
- Combination does not make sense:
  - Network Device 212 cannot directly communicate with VPN Site 806—different subnetworks
  - VPN traffic **must** be routed through “a firewall, to control access” (Ex. 1004 (Chandra) at ¶5), cannot directly communicate with another network

## Grounds 2, 6, Claims 6-7, etc. (“next network appliance”): Keohane

- Petitioner: Keohane’s “client device” is a “next network appliance”
- ‘825 Patent distinguishes “network appliances” from “endpoint devices” (client device)
- A “client device” does not meet Petitioner’s expert’s definition of “appliance”



Ex. 1004 (Keohane) at Fig. 3

“These clients 110, 112, and 114 may be, for example, personal computers or network computers.”

Ex. 1008 (Keohane) at ¶23

“The phrase ‘network appliance’ generally refers to a **specialized or dedicated device** for use on a network in virtual or physical form. ... Examples of functionality include ... Layer 2/3 routing, content inspection, content filtering, firewall ...”

Ex. 1001 (825 Patent) at 4:1-11

“[A]pppliance[s] [have] the property that they are ... devices with a small operating system that ... requires very little interaction and that does ... a **small set of specific tasks, mostly without requiring interaction.**”

Ex. 2017 (Franz Tr.) at 102:1-9

POR 53-56; Surreply 22-23

**Keohane does not render obvious updating or removing flags  
(Grounds 6, Claims 6-7, 17-18, 23-24, 28-29)**

### Summary of arguments for “updating” or “removing” flags

#### Petitioner’s Arguments

Updating or removing Keohane’s signatures obvious in view of Buruganahalli

#### Patent Owner’s Arguments

Keohane’s digital signatures authenticate the device and therefore cannot be updated/modified

Keohane requires the presence of the flags all the way to the client device, so they cannot be removed

## Ground 6, Claims 6-7, etc. (“updating” / “removing” flags)

- Claims 6-7, 17-18, 23-24, 28-29 recite “updating” or “removing” “the flag” before transmitting to a next network appliance

6. The method of claim 1, further comprising:  
updating, by the first network security appliance, the flag  
to indicate the network security operations executed by  
the first network security appliance; and  
transmitting, by the first network security network appliance, the network traffic with the updated flag to a next network appliance participating in the CSF.

7. The method of claim 1, further comprising:  
removing, by the first network security appliance, the flag  
from the network traffic; and  
transmitting, by the first network security network appliance, the network traffic without the flag to a next network appliance.

Ex. 1001 (852 Patent) at cls. 6-7

## Ground 6, Claims 6-7, etc. (“updating” / “removing” flags)

- Keohane discloses that each node appends a “digital signature” to the packet
- Petitioner alleges the “signature” is the claimed flag

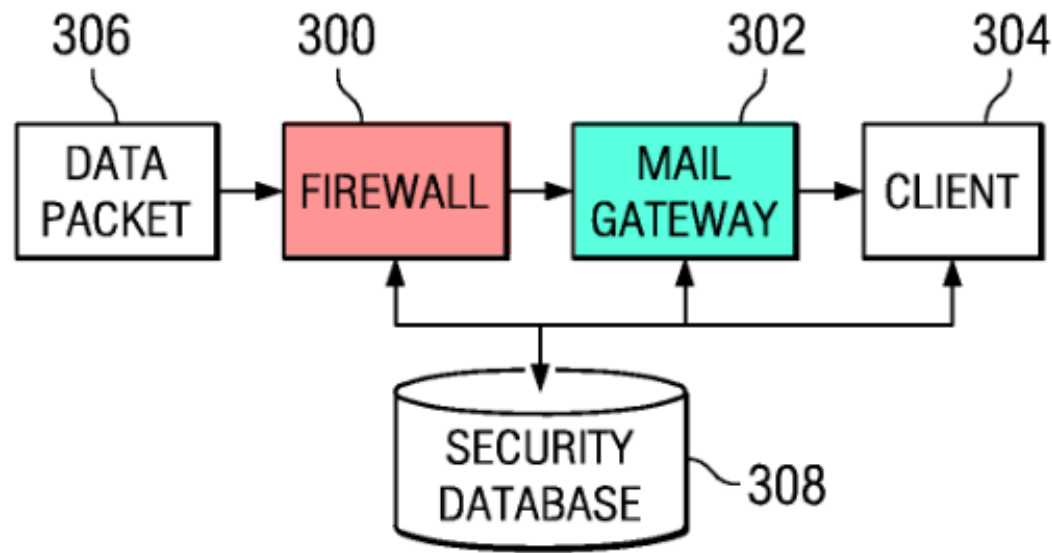


*FIG. 3*

“[T]he signature is a digital signature added to the header of data packet 306.”

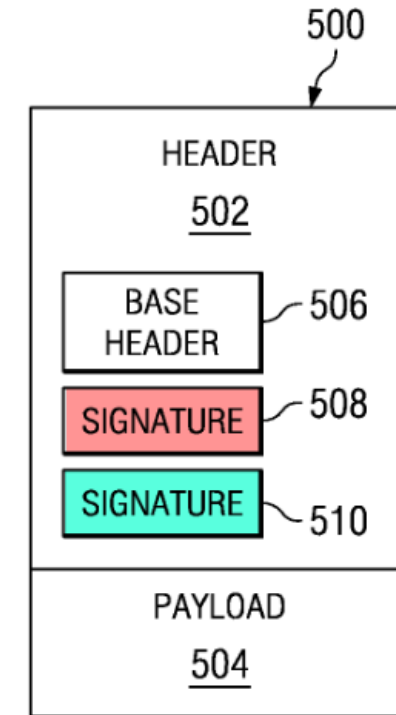


*FIG. 5*

Ex. 1008 (Keohane) at ¶34

POR 56-59; Surreply 24

## Ground 6, Claims 6-7, etc. (“updating” / “removing” flags)

- No motivation to allow signatures to be updated because a changed signature renders it useless.

“[A] POSITA would have understood that a purpose of a digital signature is to prevent tampering. This is because the very purpose of a signature is to authenticate that a message truly came from a certain sender—in Keohane’s case, the signature also authenticates which security actions were performed by the sender. Id., ¶34. If a signature could be easily altered, then the message could not be authenticated as coming from the sender.”

Ex. 2004 (Black Supp. Tr.) at ¶138

## Ground 6, Claims 6-7, etc. (“updating” / “removing” flags)

- Petitioner on Reply: obvious to share cryptographic keys between nodes and have each node “decrypt, update, and then re-encrypt the signature”
- Incorrect: exchanging keys is inefficient and not secure, as confirmed by Dr. Lee

### Exchanging keys subject to man-in-the-middle attacks

“The point is that that kind of exchange, when we do the key exchange, going through a router. So if you're not careful, the router actually remember exactly what things you are exchanging, they can actually use the same key. So there's actually a well-known attack called man in the middle.

IPR2024-00458, Ex. 2004 (Lee Tr.) at 80:23-81:21

- Each node performing decryption and encryption is more complicated and processing-intensive than Keohane’s disclosed of appending a new signature

## Ground 6, Claims 6-7, etc. (“updating” / “removing” flags)

- Petitioner on Reply: obvious to remove flags before packet is sent to client that “perform[s] no security actions”
- But Keohane discloses that all nodes can perform security actions after inspecting the signatures, even the client
  - If signature is removed, then client will perform undesirable, redundant action.

“Client 304 examines data packet 306 for signatures from trusted security elements. In this case, two signatures are found. These signatures indicate that the data packet is from a trusted source and that no viruses were found in data packet 306. Client 304 then performs an additional security action based on the security actions already performed.”

Ex. 1008 (Keohane) at ¶37