

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

---

PTAB Case No. IPR2023-00459

Patent No. 10,084,825

---

**PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 10,084,825**

---

## TABLE OF CONTENTS

### Page

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| EXHIBIT LIST .....                                                                | IV |
| I. INTRODUCTION .....                                                             | 1  |
| II. MANDATORY NOTICES .....                                                       | 1  |
| A. Real Party in Interest .....                                                   | 1  |
| B. Related Matters.....                                                           | 2  |
| C. Counsel and Service Information.....                                           | 2  |
| III. IPR REQUIREMENTS .....                                                       | 2  |
| A. Standing.....                                                                  | 2  |
| B. Challenged Claims and Relief Requested.....                                    | 3  |
| C. Prior Art.....                                                                 | 3  |
| D. Challenge Grounds .....                                                        | 3  |
| IV. TECHNOLOGY DESCRIPTION .....                                                  | 4  |
| A. Coordinated Work Existed Long Before Computers.....                            | 4  |
| B. Networked Computers Have Coordinated Their Work for<br>Decades.....            | 6  |
| C. '825 Patent Overview.....                                                      | 11 |
| 1. Alleged Invention.....                                                         | 11 |
| 2. Prosecution History.....                                                       | 16 |
| V. SECTION 325(D) ANALYSIS .....                                                  | 18 |
| VI. LEVEL OF ORDINARY SKILL .....                                                 | 19 |
| VII. CLAIM CONSTRUCTION .....                                                     | 19 |
| VIII. SPECIFIC GROUNDS.....                                                       | 19 |
| A. Ground 1: Chandra renders claims 1-5, 12, 15-16, 21-22,<br>and 27 obvious..... | 19 |
| 1. Claim 1 .....                                                                  | 22 |
| 2. Claim 2 .....                                                                  | 37 |

# **TABLE OF CONTENTS** **(continued)**

|                                                                                                    | <b>Page</b> |
|----------------------------------------------------------------------------------------------------|-------------|
| 3. Claim 3 .....                                                                                   | 39          |
| 4. Claim 4 .....                                                                                   | 40          |
| 5. Claim 5 .....                                                                                   | 43          |
| 6. Claim 12 .....                                                                                  | 43          |
| 7. Claim 15 .....                                                                                  | 44          |
| 8. Claim 16 .....                                                                                  | 45          |
| 9. Claim 21 .....                                                                                  | 45          |
| 10. Claim 22 .....                                                                                 | 46          |
| 11. Claim 27 .....                                                                                 | 46          |
| B. Ground 2: Chandra and Buruganahalli render claims 6-7,<br>17-18, 23-24, and 28-29 obvious. .... | 46          |
| 1. Motivation to Combine .....                                                                     | 50          |
| 2. Claims 6, 17, 23, 28 .....                                                                      | 50          |
| 3. Claims 7, 18, 24, 29 .....                                                                      | 57          |
| C. Ground 3: Chandra and Kumar render claims 10-11<br>obvious. ....                                | 58          |
| 1. Motivation to Combine .....                                                                     | 59          |
| 2. Claim 10 .....                                                                                  | 60          |
| 3. Claim 11 .....                                                                                  | 61          |
| D. Ground 4: Chandra and Chandra-2 render claims 13-14,<br>19-20, 25-26, and 30-31 obvious. ....   | 62          |
| 4. Claims 13, 19, 25, 30 .....                                                                     | 63          |
| 5. Claims 14, 20, 26, 31 .....                                                                     | 63          |
| E. Ground 5: Keohane renders claims 1-5, 10-12, 15-16, 21-<br>22, and 27 obvious. ....             | 64          |
| 1. Claim 1 .....                                                                                   | 69          |
| 2. Claim 2 .....                                                                                   | 79          |

# **TABLE OF CONTENTS** **(continued)**

|                                                                                                    | <b>Page</b> |
|----------------------------------------------------------------------------------------------------|-------------|
| 3. Claim 3 .....                                                                                   | 82          |
| 4. Claim 4 .....                                                                                   | 83          |
| 5. Claim 5 .....                                                                                   | 85          |
| 6. Claim 10 .....                                                                                  | 86          |
| 7. Claim 11 .....                                                                                  | 87          |
| 8. Claim 12 .....                                                                                  | 87          |
| 9. Claim 15 .....                                                                                  | 88          |
| 10. Claim 16 .....                                                                                 | 89          |
| 11. Claim 21 .....                                                                                 | 89          |
| 12. Claim 22 .....                                                                                 | 89          |
| 13. Claim 27 .....                                                                                 | 89          |
| F. Ground 6: Keohane and Buruganahalli render claims 6-7,<br>17-18, 23-24, and 28-29 obvious. .... | 90          |
| 1. Motivation to combine .....                                                                     | 90          |
| 2. Claims 6, 17, 23, 28 .....                                                                      | 91          |
| 3. Claims 7, 18, 24, 29 .....                                                                      | 94          |
| G. Ground 7: Keohane and Kumar render claims 10 obvious. ....                                      | 96          |
| 1. Motivation to Combine .....                                                                     | 96          |
| 2. Claim 10 .....                                                                                  | 96          |
| H. Ground 8: Keohane and Chandra-2 render claims 13-14,<br>19-20, 25-26, and 30-31 obvious. ....   | 97          |
| 1. Claims 13, 19, 25, 30 .....                                                                     | 98          |
| 2. Claims 14, 20, 26, 31 .....                                                                     | 98          |
| IX. CONCLUSION.....                                                                                | 99          |
| <b>LISTING OF CHALLENGED CLAIMS.....</b>                                                           | <b>100</b>  |

## EXHIBIT LIST

|          |                                                                          |
|----------|--------------------------------------------------------------------------|
| Ex. 1001 | U.S. Patent No. 10,084,825 to Xu (“the ’825 patent”)                     |
| Ex. 1002 | Supporting Declaration of Dr. Michael Franz (“Franz”)                    |
| Ex. 1003 | File History of U.S. Patent No. 10,084,825                               |
| Ex. 1004 | U.S. Patent Application Publication 2007/0204018 A1 (“Chandra”)          |
| Ex. 1005 | U.S. Patent Application Publication 2014/0282843 A1<br>(“Buruganahalli”) |
| Ex. 1006 | U.S. Patent Application Publication 2009/0144818 A1 (“Kumar”)            |
| Ex. 1007 | U.S. Patent Application Publication 2017/0093917 A1<br>(“Chandra-2”)     |
| Ex. 1008 | U.S. Patent Application Publication 2008/0134332 A1 (“Keohane”)          |
| Ex. 1009 | Microsoft Computer Dictionary Fifth Edition (2002)                       |
| Ex. 1010 | U.S. Patent Publication 2006/0156401 A1 (“Newstadt”)                     |
| Ex. 1011 | U.S. Patent Publication 2007/0237147 A1 (“Quinn”)                        |

## **I. INTRODUCTION**

U.S. Patent No. 10,084,825 (“the ’825 patent”) takes an ancient idea, applies it to computers, and does so identically to countless prior systems to which the Examiner did not have access.

For as long as humans have collaborated, segregating tasks and avoiding repetition has been a desirable approach. Any number of well-worn phrases—“dividing and conquering,” “staying in your lane”—reflect the common-sense notion that output can be optimized by coordinating multiple actors performing multiple tasks.

Networked computers have long benefited from coordination. Consequently, throughout the early 2000s, industry leaders like McAfee, IBM, and Symantec developed coordinated firewalls, routers, and other network components. Unfortunately, none of this was considered during prosecution of the ’825 patent.

Now that Netskope, Inc. (“Petitioner”) has identified those references not considered during prosecution, the Board will see that the ’825 patent’s “Cooperative Security Fabric” is nothing more than a rehash of prior techniques. Accordingly, IPR should be instituted against claims 1-7 and 10-31 and those claims cancelled for the reasons stated below.

## **II. MANDATORY NOTICES**

### **A. Real Party in Interest**

Netskope, Inc. is the sole real party-in-interest.

## **B. Related Matters**

Petitioner has filed a civil action seeking a declaratory judgment that it does not infringe the '825 patent in *Netskope, Inc. v Fortinet, Inc.*, No. 3:22-CV-01852-TLT (N.D. Cal.). That case is currently stayed. Petitioner has challenged the validity of other patents allegedly owned by the Patent Owner in six co-pending *inter partes* review proceedings. (See IPR2022-01587, IPR2023-00030, IPR2023-00175, IPR2023-00456, IPR2023-00457, IPR2023-00458).

## **C. Counsel and Service Information**

Lead counsel: Thomas N. Millikan (Reg. No. 72,316).

Back-up counsel: Babak Tehranchi (Reg. No. 55,937), Andrew N. Klein (*pro hac vice* forthcoming) and Bingjie (Kay) Li (*pro hac vice* forthcoming).

These attorneys can be reached by mail at Perkins Coie LLP, 11452 El Camino Real, Suite 300, San Diego, California, 92130, by phone at (858) 720-5700 and by fax at (858) 720-5799.

Petitioner consents to electronic service. All services and communications to the attorneys listed above may be sent to:

**Netskope-FortinetIPRTeam@perkinscoie.com.**

A Power of Attorney for Petitioner is being filed concurrently.

## **III. IPR REQUIREMENTS**

### **A. Standing**

The '825 patent is available for IPR and Petitioner is not barred or estopped

from challenging the claims on the grounds herein.

**B. Challenged Claims and Relief Requested**

Petitioner requests cancellation of the challenged claims under §103.

**C. Prior Art**

Petitioner relies on the references listed in the Table of Exhibits, including:

- U.S. Patent Application Publication 2007/0204018 A1  
 (“Chandra”) (Ex. 1004)
- U.S. Patent Application Publication 2014/0282843 A1  
 (“Buruganahalli”)
- U.S. Patent Application Publication 2009/0144818 A1  
 (“Kumar”)
- U.S. Patent Application Publication 2017/0093917 A1  
 (“Chandra-2”)
- U.S. Patent Application Publication US 2008/0134332 A1  
 (“Keohane”) (Ex. 1008)

All references are prior art under §102(a)(1). Petitioner also relies on the declaration of Dr. Michael Franz (“Franz” (Ex. 1002)).

**D. Challenge Grounds**

| Ground | Basis | Reference(s) | Challenged Claims         |
|--------|-------|--------------|---------------------------|
| 1      | §103  | Chandra      | 1-5, 12, 15-16, 21-22, 27 |

|   |      |                            |                              |
|---|------|----------------------------|------------------------------|
| 2 | §103 | Chandra + Buruganahalli    | 6-7, 17-18, 23-24, 28-29     |
| 3 | §103 | Chandra + Kumar            | 10-11                        |
| 4 | §103 | Chandra + Chandra-2        | 13-14, 19-20, 25-26, 30-31   |
| 5 | §103 | Keohane                    | 1-5, 10-12, 15-16, 21-22, 27 |
| 6 | §103 | Keohane +<br>Buruganahalli | 6-7, 17-18, 23-24, 28-29     |
| 7 | §103 | Keohane + Kumar            | 10                           |
| 8 | §103 | Keohane + Chandra-2        | 13-14, 19-20, 25-26, 30-31   |

#### **IV. TECHNOLOGY DESCRIPTION**

##### **A. Coordinated Work Existed Long Before Computers**

Coordinating work was a well-known concept inside and outside computer networking long before the '825 patent. The picture below, for example, shows a 1943 routing slip used when distributing an ordinance pamphlet to the U.S. Pacific Fleet.

ComServPac—S-9-43—5M—1897.

**UNITED STATES PACIFIC FLEET  
SERVICE SQUADRON SIX  
ROUTING SLIP**

Routing Slip No. **2578**

From: Buord  
Subject: 0.50-inch Machine Gun Mounts Mark 17 Mods. 1  
And 2.

File No. -- Serial No. --  
Dated: 8/43 Date Received 9/15  
Our File: EN6(6) Filed:  
No. Copies Recd. 2 For Distr.:

| Referred to                  | For        | Initial           | Remarks                                |
|------------------------------|------------|-------------------|----------------------------------------|
| 00 Comseron SIX              | ✓          | <i>[initials]</i> |                                        |
| 11 Operations<br>Gun. & WP   | ✓          | <i>[initials]</i> |                                        |
| 20 Communications            | ✓          | <i>[initials]</i> |                                        |
| 70 Engineering &<br>Material | ✓          | <i>[initials]</i> |                                        |
| 50 Degaussing                | ✓          | <i>[initials]</i> |                                        |
| 60 Personnel                 |            |                   |                                        |
| 90 Mining                    | ✓          | <i>[initials]</i> |                                        |
| 05 Secretary                 |            |                   |                                        |
| Cominron                     |            |                   |                                        |
| Yeoman <u>20</u>             | <u>1-6</u> | <i>[initials]</i> | <i>Copy filed in<br/>Conf. Cabinet</i> |

All correspondence will be read and returned to the Flag Secretary promptly. Attach replies and basic correspondence hereto. No correspondence will be taken out of the office without authority of the Secretary.

|                |                                 |                                          |
|----------------|---------------------------------|------------------------------------------|
| 1. Action      | 5. Investigation                | 8. For publication to Squadron           |
| 2. Information | 6. Make correction              | 9. Make recommendations                  |
| 3. Compliance  | 7. Retain copy and routing slip | 10. Prepare reply for 60<br>signation by |
| 4. Comment     |                                 |                                          |

The slip shows different departments received the material for different reasons. After completing their respective tasks, parties signed to certify compliance, then passed the slip to the next department. In addition to predetermined tasks, the routing slip even allows for action items to be added during the process (“copy filed

in conf. cabinet”). Thus, any given recipient could verify what work had already been performed and skip previously-completed tasks. (Franz, ¶¶36-37.)

**B. Networked Computers Have Coordinated Their Work for Decades**

By the early 2000s, collaboration between security devices protecting a network was widespread. Specifically, as companies found themselves purchasing a hodgepodge of devices to secure increasingly-complex networks—virus detectors, firewalls, routers—coordination was imposed to increase efficiency and reduce duplication.

Each reference below predates the ’825 patent by over a decade and shows coordinated action between devices using flags/policies:

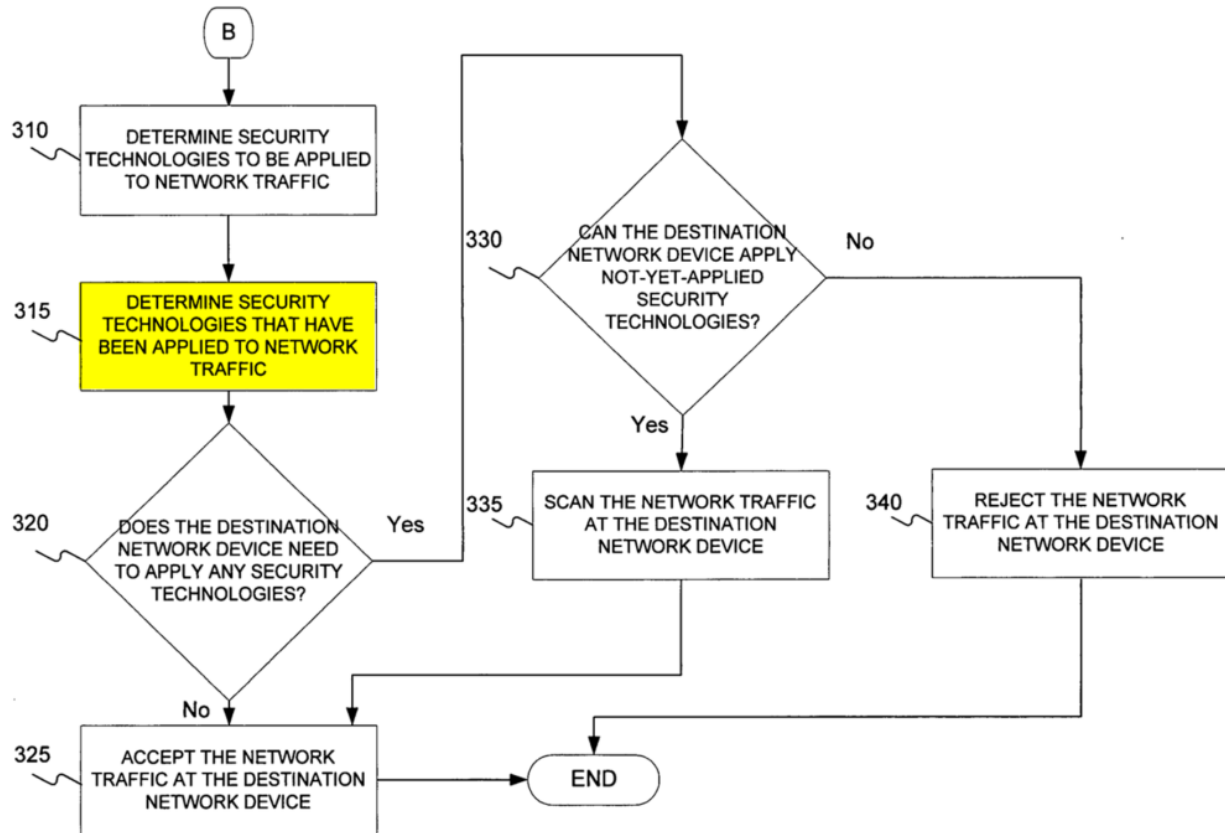


Fig. 3 (Annotated)

(Newstadt, filed January 2005.)

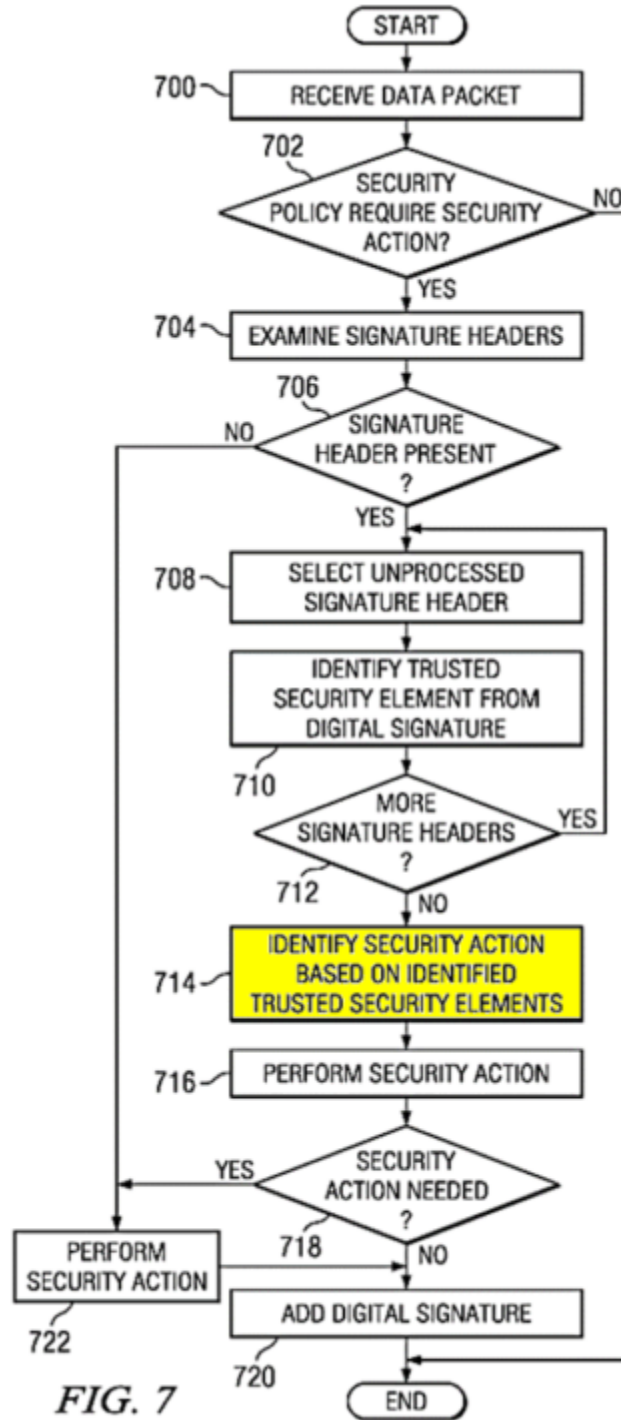
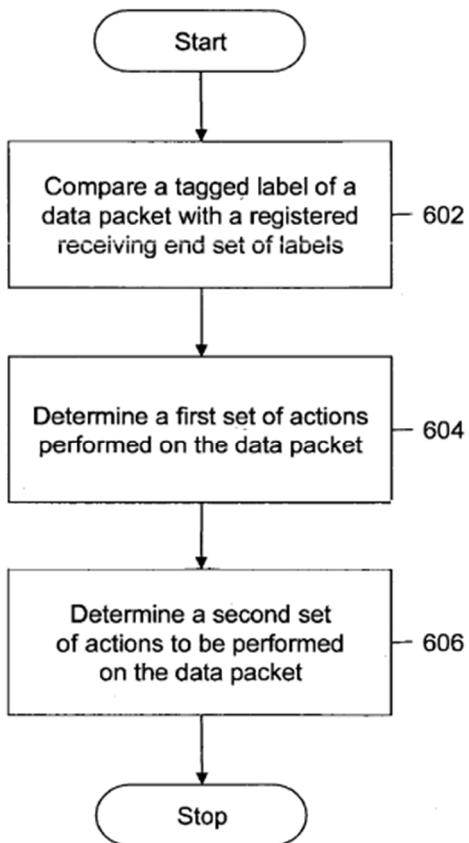


FIG. 7  
(Annotated)

(Keohane, filed December 2006.)



(Chandra, filed February 2006.)

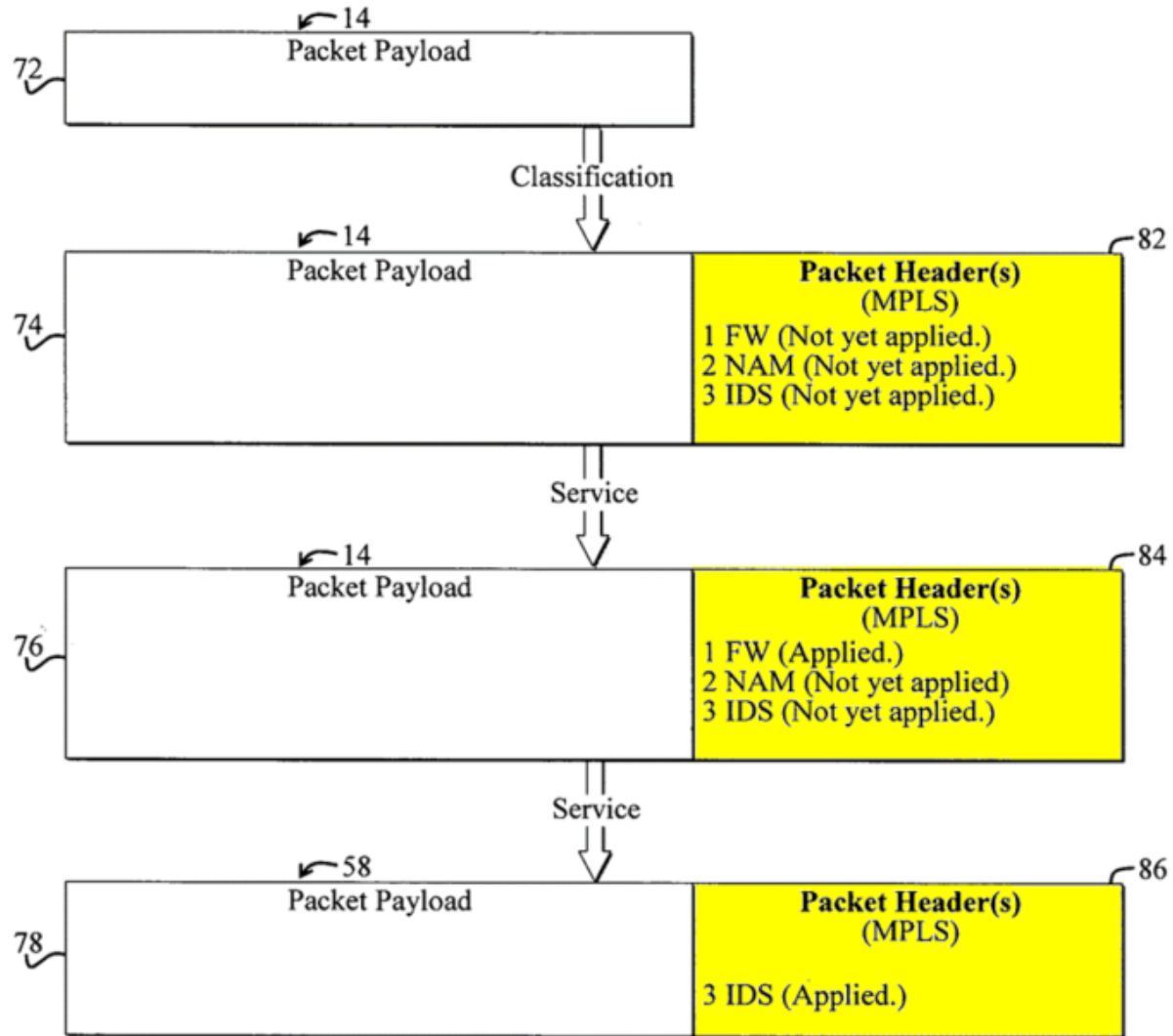


**Fig. 2 (Annotated)**

(Quinn, filed 2006.)

These references track operations by indicating them in packets that move between devices. Network packets are typically composed of a “header” and a “payload.” The header contains routing information as well as space for additional

information such as “flags” and other fields. Like the entries on the 1940s routing slip depicted above, these flags and fields allow security devices to denote what tasks have been completed with respect to a particular packet of information, so that downstream devices can understand and account for those tasks.

For example, Quinn (shown immediately above) disclosed using packet headers to specify actions to be performed as a packet progressed through network appliances and updating the header to reflect that progress.<sup>1</sup>

As another example, Newstadt—filed in 2005— disclosed placing a security marker in a packet header. The marker could include the security technologies that had (or had not) been applied to the network traffic. The security marker could be authenticated using a public key scheme, like Public Key Infrastructure. Downstream devices used the header information to determine which operations to perform.

## **C. '825 Patent Overview**

### **1. Alleged Invention**

The '825 patent concerns “coordinating security operations among members of a cooperative security fabric (CSF)...” ('825 patent, 2:3-5.)

Figure 1 (below) depicts an exemplary architecture according to an '825

---

<sup>1</sup> Quinn, ¶¶39-50.

embodiment. The architecture includes a private network (120) that has appliances (e.g., network security appliances (121, 130a and 130b, 140a-140d)) and subnets (141a-141d). The exemplary architecture also includes subnet (151) and subnet network security appliance (150), which connect to private network (120) through an Internet-based virtual private network (VPN). (*Id.*, 4:58-67.) The '825 patent explains that “subnet 151 and subnet network security appliance 150 may be seen as a part of private network 110 [*recte* 120].” (*Id.*, 5:1-2.)

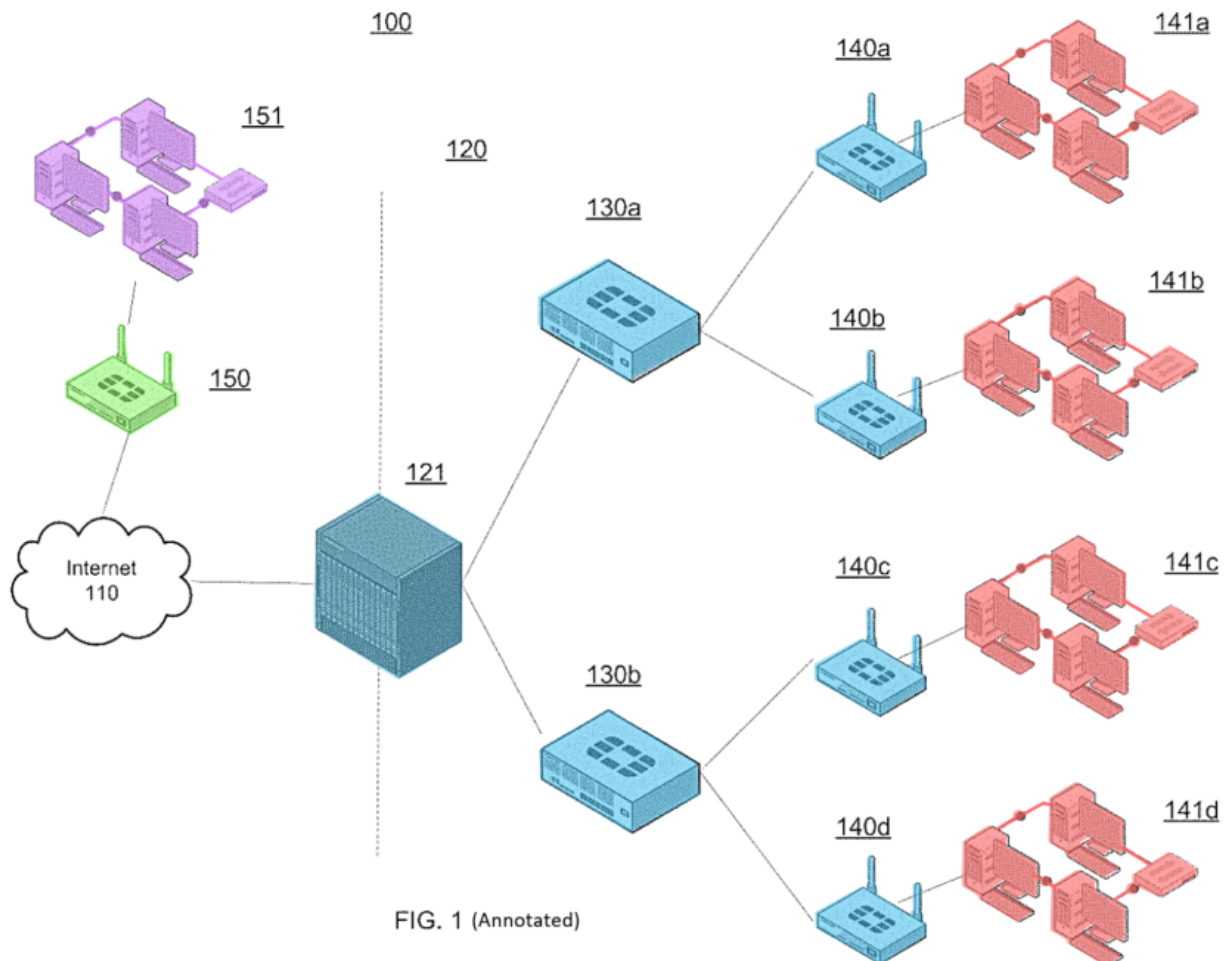


Figure 2 (below) depicts a topology of Figure 1's network appliances. The '825 patent describes the network appliances' position in the architecture using a tree analogy: root node (220) corresponds to network security appliance (121), branch nodes (230a, 230b) correspond to network security appliances (130a, 130b) and leaf nodes (240a-240d) correspond to network security appliances (140a-140d). (*Id.*, 5:52-53, 60-62, 6:1-3.) The '825 patent explains that a POSITA would appreciate that the topology could include other combinations of "roots," "branches," and "leaves." (*Id.*, 6:14-16.) For example, the topology could involve as few as two network security appliances, "such as the network path in which a leaf node 250 is connected to root node 220 directly." (*Id.*, 6:16-20.) Together, the network security appliances "form a cooperative security fabric that coordinates operations among members and avoids redundant operations." (*Id.*, 5:45-47.) The '825 patent does not give the "cooperative security fabric (CSF)" a reference numeral, but rather simply describes the CSF as the result of appliances coordinating security operations performed on network traffic passing through them.

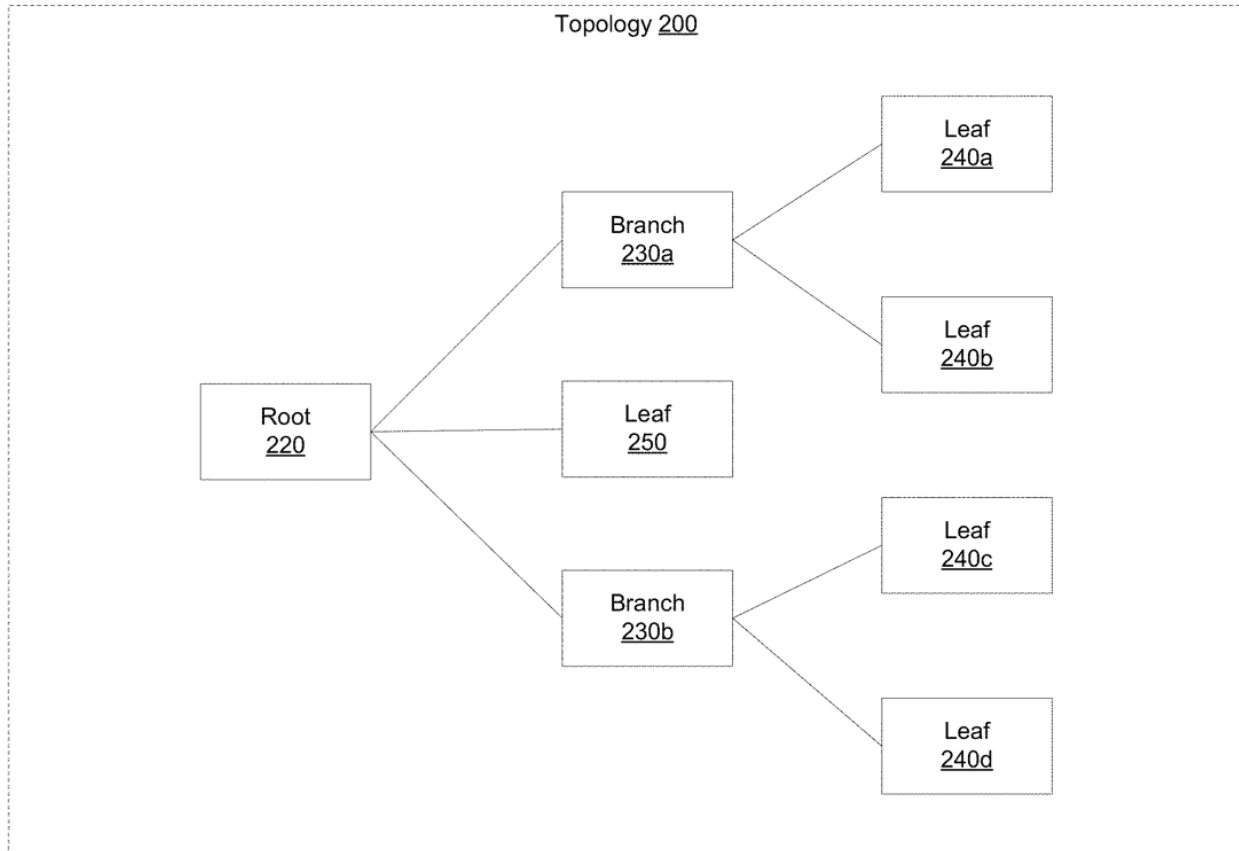


FIG. 2

In operation, a network appliance “may add one or more flags (e.g., a single bit flag or a collection of bit fields) to a network packet after it is inspected by the member node” and may transmit the network packet with the flag “to another member node at the next hop.” (*Id.*, 6:28-34.) The flag may be added to the header of the network packet (similar to Quinn, Newstadt, and Keohane, as discussed above). (*Id.*, 9:29-32.) Once that next-hop member node receives the network packet, it “may check if the flag is carried by the network packet” and, if so, it “may determine to skip the operations that have been reported via the flag(s) as having

been executed by the last member node.” (*Id.*, 6:34-39.) This coordination replicates both the 1943 routing slip and the patented inventions discussed above. Figure 3 (below) illustrates this workflow. (*Id.*, 6:49-8:41.)

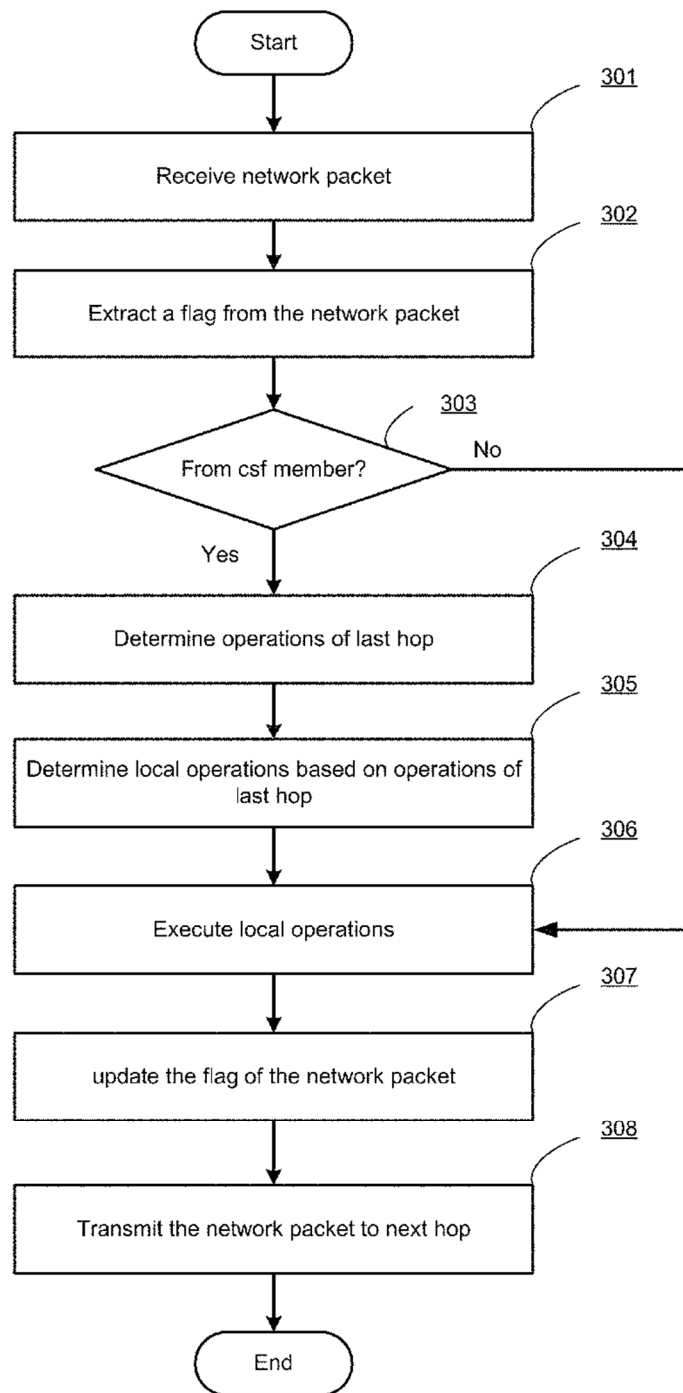


FIG. 3

## 2. Prosecution History

Prosecution involved only a single office action and a scant six references, all

of which were found by the examiner. (Ex. 1003, 63.) In the lone office action, the examiner rejected then-pending claims 1, 5, and 11-15 as anticipated by U.S. Patent No. 9,054,990 (“Davis”) and claims 2-4 and 6-10 for depending from a rejected base claim. But the examiner explained that claims 2-4 and 6-10 would be allowable if rewritten as independents. (Ex. 1003, 59-61.)

In response, Applicant amended claim 1 to incorporate claim 2 and created three new independent claims, each of which combined claim 1 with a different dependent. Specifically, amended claim 1 added the already-obvious limitation shown in underline:

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. 1003, 78-79.) A table provided by Applicant shows the overlap between the claims. (See Ex. 1003, 78-86.)

| New/Amended Claims | Corresponding Former Claims |
|--------------------|-----------------------------|
| 1                  | 1 + 2                       |
| <b>16</b>          | 1 + 3                       |
| 17 through 19      | 6 through 8                 |
| 20 through 21      | 14 through 15               |
| <b>22</b>          | 1 + 4                       |
| 23 through 25      | 6 through 8                 |
| 26 through 27      | 14 through 15               |
| <b>28</b>          | 1 + 6                       |
| 29 through 30      | 7 through 8                 |
| 31 through 32      | 14 through 15               |

After the amendment, the examiner allowed the claims. (Ex. 1003, 94.)

## V. SECTION 325(D) ANALYSIS

The Board should institute IPR notwithstanding its discretion under §325(d). *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (P.T.A.B. Dec. 15, 2017) (identifying six-factor test); *Advanced Bionics, LLC v. Med-El Electromedizinische Geräte GMBH*, IPR2019- 01469, Paper 6 at 10 (P.T.A.B. Feb. 13, 2020) (precedential).

Factors (a), (b), and (d): None of the Petition's references were before the examiner. (Ex. 1003.) Accordingly, the Petition does not present the same/substantially the same art or arguments previously presented to the USPTO.

Factors (d), (e) and (f): The combinations below present new and distinct invalidity challenges that better reflect the state of the prior art than what was considered during original examination. These grounds show fatal defects in the challenged claims the examiner did not consider.

## **VI. LEVEL OF ORDINARY SKILL**

As of the '825 patent's filing date, a POSITA would have had at least a B.S. degree in computer science, computer engineering, or electrical engineering (or equivalent experience) and would have had at least two years' practical experience with computer networking and computer security. (*See* Franz, ¶28.)

## **VII. CLAIM CONSTRUCTION**

The challenged claims should be construed “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. §42.200(b); *see Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). Petitioner does not believe claim construction is necessary.

## **VIII. SPECIFIC GROUNDS**

### **A. Ground 1: Chandra renders claims 1-5, 12, 15-16, 21-22, and 27 obvious.**

**Chandra:** Over a decade before the '825 patent, Chandra recognized that network appliances not coordinating operations would cause redundant actions and waste resources. (Chandra, ¶¶4-7.) Also, much like the '825 patent, Chandra disclosed an invention addressing that problem wherein network appliances coordinated operations using labels passed between appliances. (Chandra, Abstract, ¶30.)

Chandra's Figure 2 (below) depicted an embodiment that consisted of a

transmitting end (202) and a receiving end (204), each of which included a network device (206, 212), a Customer Edge (CE) (208, 214), and a Provider Edge (PE) (210, 216). (*Id.*, ¶¶24-26.)

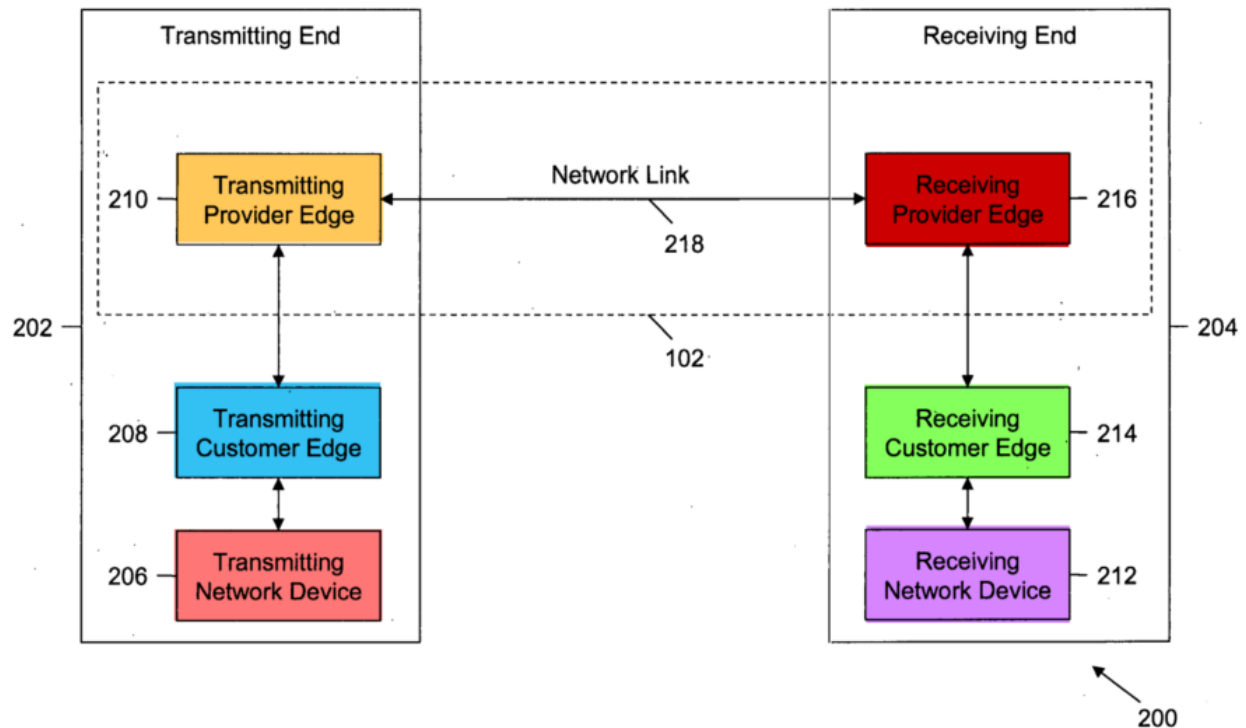


FIG. 2 (Annotated)

Transmitting CE (208) and receiving CE (214) were security-based devices, like “Intrusion Detection Systems (IDSs), fire walls, etc.,” that performed security actions on a data packet. (*Id.*, ¶30.)

At setup, transmitting CE (208) and receiving CE (214) authenticated each other and exchanged an identical set of “CE labels to be used for tagging [] data packets.” (*Id.*, ¶¶33, 34.) Transmitting CE (208) and receiving CE (214) then each registered and stored the labels in a table. (*Id.*, ¶52.) The tables below depicted

exemplary labels used to coordinate actions performed on a data packet. The receiving CE labels were associated with the address of transmitting CE (208).

|                           |            |               |                                |
|---------------------------|------------|---------------|--------------------------------|
| Transmitting<br>CE labels |            |               |                                |
|                           | 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    |
| Receiving<br>CE labels    | ...        |               |                                |
|                           | 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 |
|                           | ...        |               |                                |

(*Id.*, ¶¶51-52.) Transmitting CE used the labels to indicate a first set of actions it had performed on network traffic, while receiving CE used them to determine the actions previously performed by transmitting CE and to determine the actions it needed to perform. (*Id.*)

In operation, transmitting network device (206) sent a packet to transmitting CE (208). Then, transmitting CE 208 “perform[ed] a first set of actions on the data packet, and tag[g]ed the data packet with a CE label indicating the first set of actions that ha[d] been performed.” (*Id.*, ¶31.) Transmitting CE (208) transmitted the tagged data packet to receiving CE (214) through transmitting PE (210) and receiving PE (216). (*Id.*, ¶¶31-32.) Receiving CE (214) analyzed the label to

identify the first set of actions performed by transmitting end (202) and determine a second set of actions to perform on the data packet. (*Id.*)

For example, using the exemplary CE labels above, if transmitting CE (208) performed security actions corresponding to rules A and B on the data packet, it would tag the data packet with a label 1256. “When this tagged data packet reache[d] receiving CE [], receiving CE [] refer[red] to the receiving CE table, and determine[d] that actions corresponding to rules A and B ha[d] been performed on the data packet by transmitting CE []. Therefore, receiving CE [] [could] obviate th[o]se redundant actions.” (*Id.*, ¶53.)

## 1. Claim 1

### a. 1[pre]: “A method comprising:”

Chandra disclosed a “method that enable[d] the obviation of [] redundant actions by tagging a data packet with a label indicating a first set of actions performed on the data packet at a transmitting end.” (*Id.*, ¶18.)

### b. 1[a]: “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;”

Chandra disclosed a receiving CE (first network security appliance) of a private network (e.g., a local area network or Virtual *Private Network*) that coordinated security actions with other appliances and received and inspected data packets (network traffic).

**“first network security appliance of a private network”**: Chandra disclosed a first network security appliance in the form of a receiving CE.

Figure 2 (below) depicted a **receiving CE (214)** that could be a “security-based device.” (Chandra, ¶30.) For example, **receiving CE (214)** could be “Intrusion Detection Systems (IDSs), fire walls, etc.” (*Id.*, ¶30.) A POSITA would have found it obvious that IDSs and firewalls were network security appliances because they were well-known devices that performed network security operations. The ’825 patent, for example, broadly discloses examples of network security appliances, including the Fortigate firewall device. (’825 patent, 4:16-18; Franz, ¶65.)

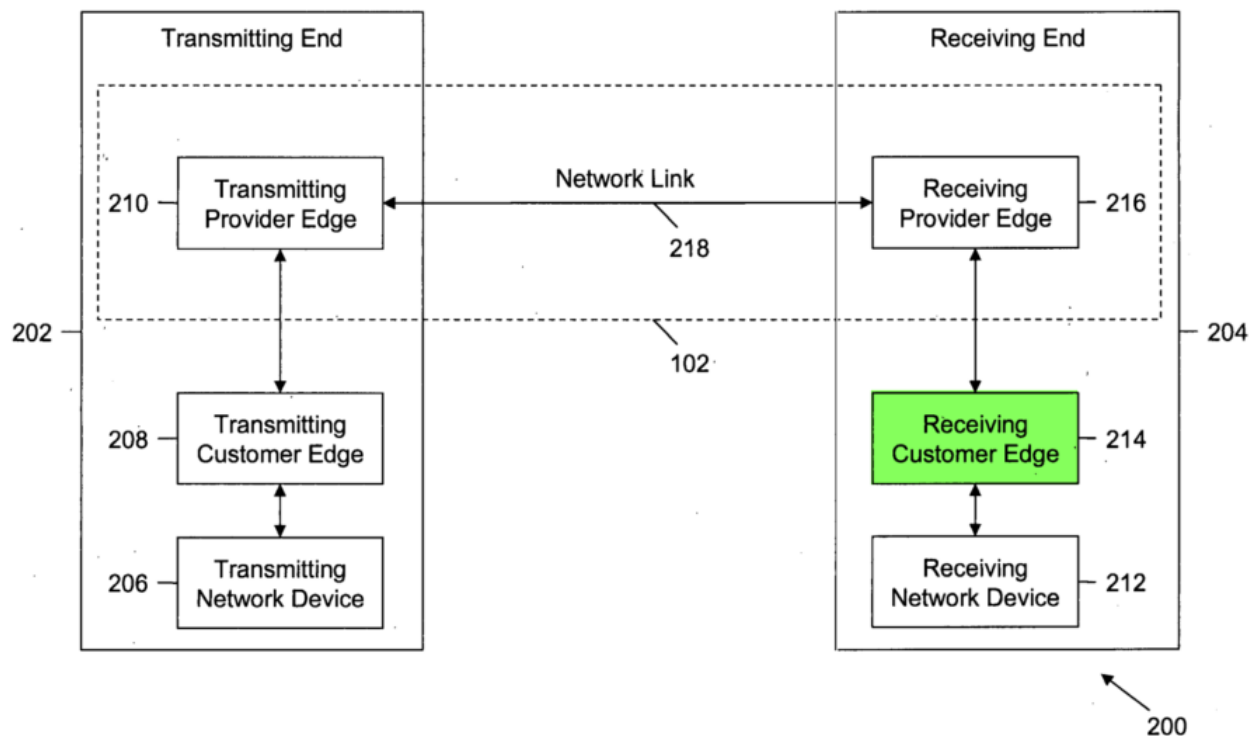


FIG. 2 (Annotated)

Chandra also disclosed that the receiving CE could be implemented in a

private network, like a local network or virtual private network. Chandra explained that network (102) (shown above) “provide[d] a communication medium to network devices [] for data to be transmitted from one network device to another network device” and could be, for example, a Local Area Network (LAN). (Chandra, ¶21.) A POSITA would have found it obvious that a LAN could be a private network because, long before the ’825 patent, LANs (e.g., an enterprise network) were commonly setup as private networks using private network addresses. (Franz, ¶66.)

Additionally, Chandra explained that its invention—including the receiving CE—could be implemented in a Virtual *Private Network*. (Chandra, ¶¶4-7, 58-68, Fig. 8.) Chandra explained that a VPN included “a security device, such as a firewall, to control access.” (*Id.*, ¶5.) As an example, Chandra’s Figure 8 (below) illustrated elements of such a system where the transmitting and receiving CEs were parts of a private network that used an encrypted, private tunnel connecting two ends of communication. (Franz, ¶67.)

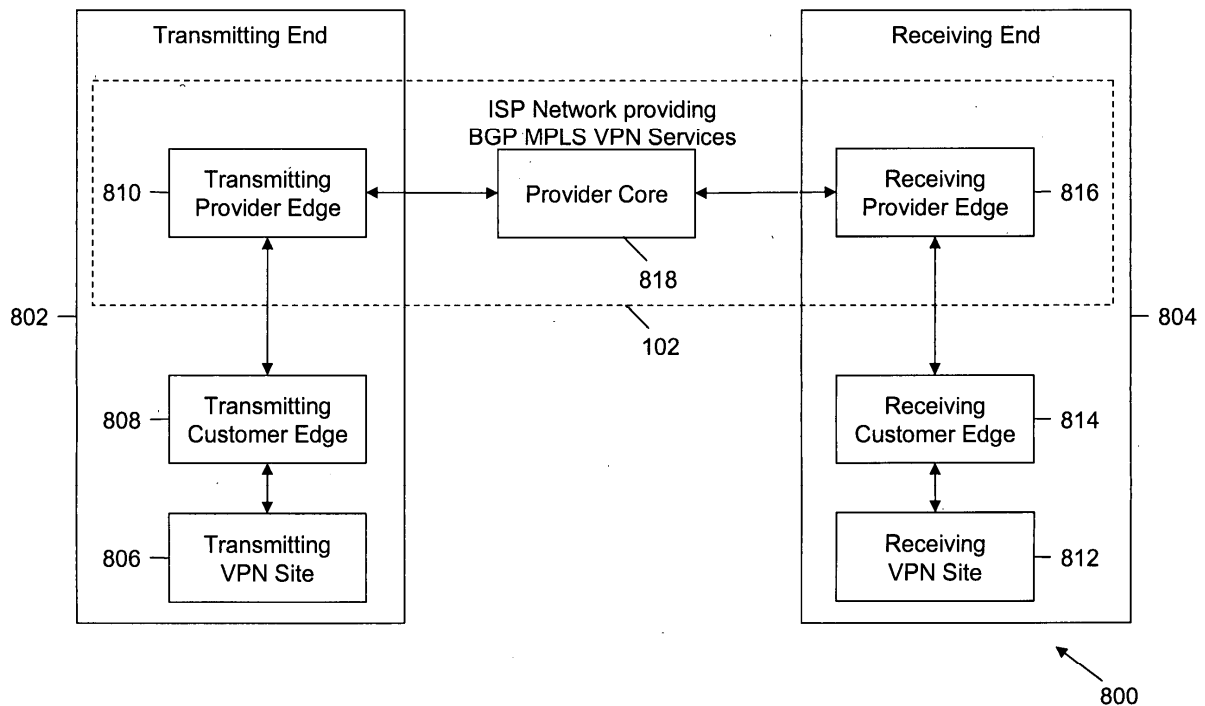
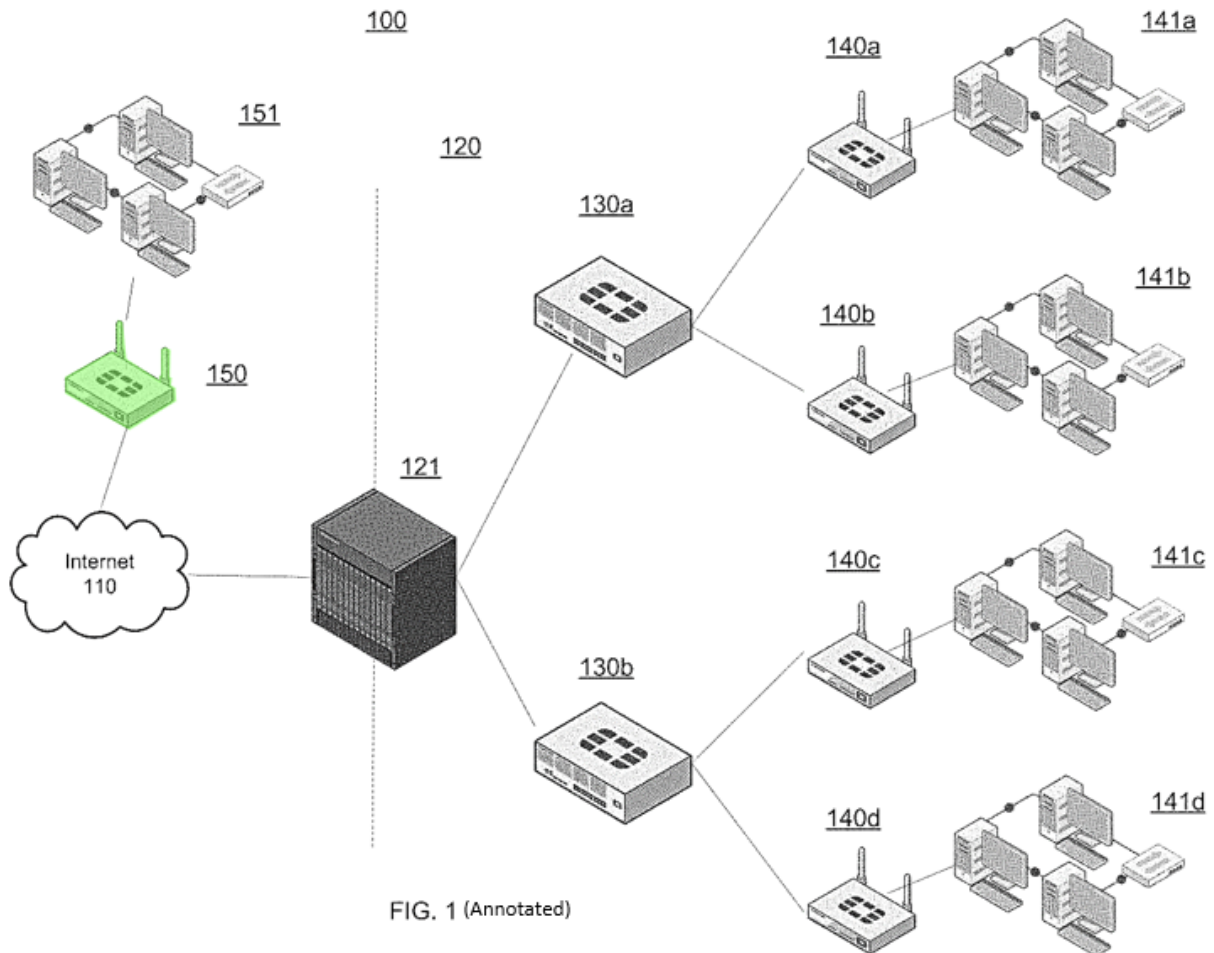


FIG. 8

The '825 patent similarly discloses a VPN can be a private network. Figure 1 (below) depicted “a subnet 151 and a **subnet network security appliance 150** [] connected to private network 120 through the Internet 110 via VPN.” ('825 patent, 4:65-67.) Subnet (151) and **subnet network security appliance (150)**, according to the '825 patent, “may be seen as part of private network 110.” (*Id.*, 5:1-2.) This is consistent with Chandra. For example, transmitting VPN site could be a private enterprise network and receiving VPN site could be a remote employee’s computer connecting back to the enterprise network or the subnet of a branch office connecting back to the main enterprise network, and vice versa. The receiving CE, like

appliance 150 in Figure 1, would be part of the private network. Thus, a POSITA would have found it obvious that a device (e.g., a receiving CE) operating in a VPN would be on a private network. (Franz, ¶¶68.)



**“participating in a cooperative security fabric (CSF)”**: Chandra disclosed that receiving CE (214) cooperated with transmitting CE (208) to coordinate security actions performed on network traffic. (Chandra, Abstract, ¶¶18, 24-26, 30.) At setup, receiving CE (214) and transmitting CE (208) authenticated each other and

exchanged labels that could be used to coordinate security actions. (*Id.*, ¶¶19-20, 33-34.) This exchange of information enabled coordinated enforcement of rules, which helped obviate redundant operations. (*Id.*, ¶¶18-20.)

Chandra's disclosures align with the '825 patent's discussion about the CSF. The '825 describes the CSF primarily by what it achieves—it “coordinates operations among members and avoids redundant operations.” ('825 patent, 5:45-47, 1:64-68.) As discussed, that is precisely what the cooperative transmitting and CEs achieve. Moreover, the '825 patent does not set a minimum number of appliances needed to form a CSF and, in fact, explains that as few as two are needed. (*See, e.g., id.*, 6:18-20.) Therefore, Chandra disclosed that receiving CE participated in a CSF. (Franz, ¶¶69-70.)

**“receiving...network traffic that is to be inspected by the first network security appliance”**: Chandra disclosed that receiving CE received network traffic (data packets) before inspecting it. (Chandra, ¶¶32 (“Next, receiving PE 216 ***transmits the tagged data packet to receiving CE 214***. Receiving CE 214 pops off the tagged CE label. Based on this CE label, receiving CE 214 identifies the first set of actions. According to the identified first set of actions, receiving CE 214 determines a second set of actions that has to be performed on the data packet.”)<sup>2</sup>,

---

<sup>2</sup> All emphases herein are Petitioner's, unless otherwise noted.

37, 46 (“*On receiving the data packet...*receiving CE 214 compare[d] the CE label tagged on the data packet with the registered receiving end set of labels.”).)

- c. **1[b]: “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;”**

Chandra disclosed that receiving CE (first network security appliance) determined whether network traffic had been transmitted from a transmitting CE (second network security appliance) using a label (flag) carried by the packet.

As explained above, in Chandra the transmitting and receiving CEs authenticated each other and exchanged labels for coordinating security operations. (Chandra, ¶¶31-35.) The CE labels were exchanged and registered because “receiving CE 214 need[ed] to recognize the CE label.” (*Id.*, ¶47.) Once transmitting CE (208) received network traffic from a **transmitting network device (206)**, it performed a first set of actions on the traffic “and tag[ged] the data packet with a CE label indicating the first set of actions that ha[d] been performed.” (*Id.*, ¶31.) The network traffic then travelled from **transmitting CE (208)** to **transmitting PE (210)** to **receiving PE (216)** and, finally, to **receiving CE (214)**. (*Id.*, ¶¶31-32.)

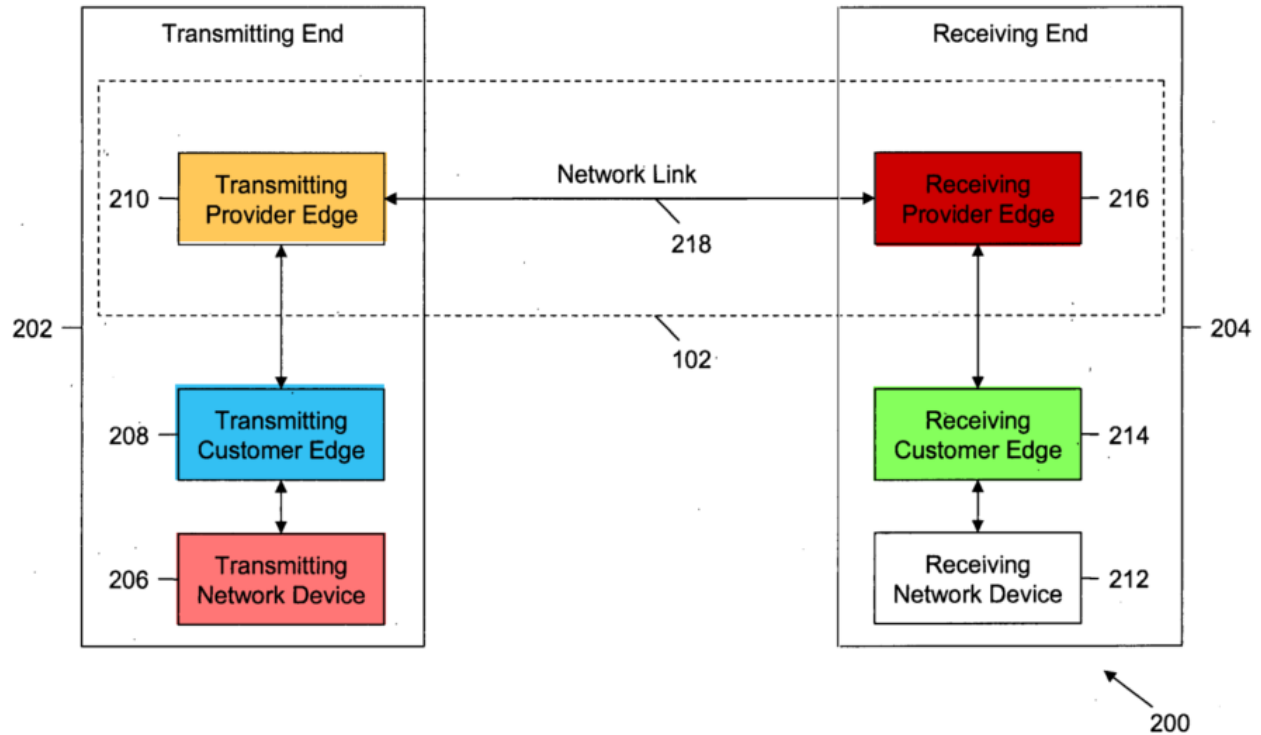


FIG. 2 (Annotated)

Once receiving CE received network traffic, it “checked *if the data packet ha[d] been tagged with a CE label* present in the registered receiving end set of labels.” (*Id.*, ¶48; *see also, e.g.,* ¶¶46, FIGs. 6-7.) This was depicted in [step 602](#), below.

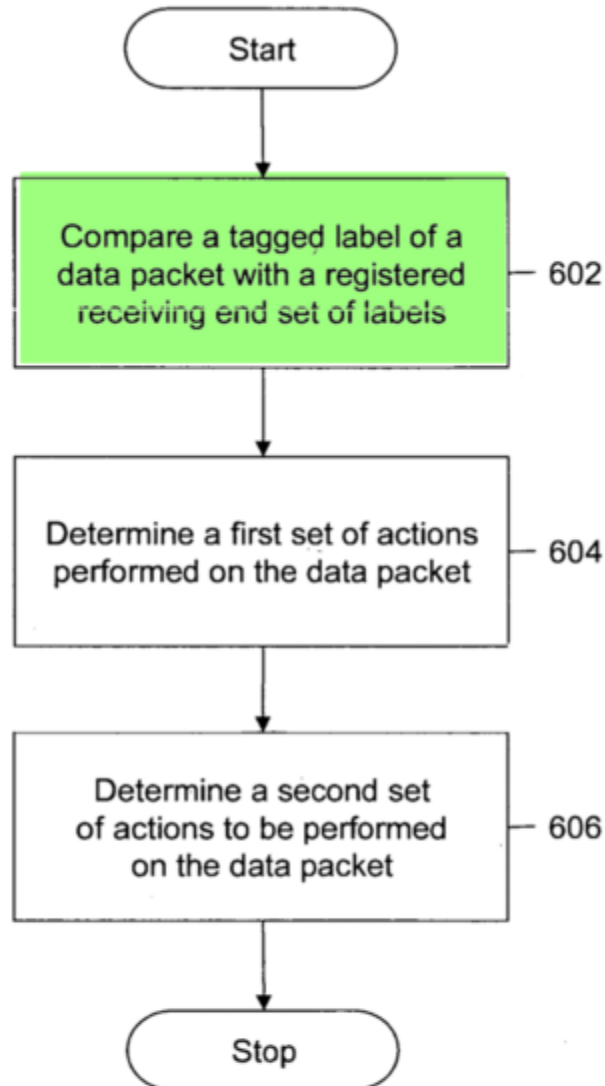


**FIG. 6** (Annotated)

In other words, receiving CE determined if the packet had a CE label that corresponded to one previously exchanged with the transmitting CE (a second security appliance participating in the CSF). (*Id.*, ¶47-48.) This was done because

network traffic could have “not been tagged with a CE label or the tagged CE label [was] not recognizable by receiving CE 214,” in which case a separate set of actions was done. (*Id.*, ¶¶47-49; *see also, e.g., id.*, ¶37 (“At step 306, receiving CE 214 identifie[d] the CE label. This CE label [was] present in the registered receiving end set of labels, and therefore, [could] be recognized by receiving CE 214.”).) Thus, because each CE label used by transmitting CE (208) to tag the data packet was registered at receiving CE (214), a POSITA would find it obvious that when receiving CE (214) checked the data packet for a label (flag), the presence of a registered CE label in the data packet indicated that the data packet had been transmitted from transmitting CE (208). This is consistent with the ’825 patent’s disclosure that a flag’s presence on network traffic serves as “an indicator to subsequent member nodes along the transmission path that...the incoming packet was transmitted from the member node.” (’825 patent, 6:54-59, 6:65-67.) Receiving CE (214) could also look up the CE label, which was associated with the address of transmitting CE (208), in the registered label table (below) to further confirm that the data packet was transmitted from transmitting CE (208). (Franz, ¶76.)

| 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 |
| ...        |               |                                |

Additionally, the CE label was a number such as “1256” or “1257.” (Chandra,

¶52.) A POSITA would find it obvious that the CE label was a flag because the '825 patent described the recited “flags” broadly, e.g., “a single bit flag or a collection of bit fields.” ('825 patent, 6:28-34, Franz, ¶77.)

- d. 1[c]: “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;”

Chandra disclosed that, once the receiving CE (first network security appliance) determined that the data packet (network traffic) had been transmitted from the transmitting CE (second network security appliance), it determined the security operations performed by the transmitting CE. Specifically, for [step 604](#) in Figure 6 (below), Chandra disclosed that “the *first set of actions performed on the data packet at transmitting CE 208 [was] determined.*” (Chandra, ¶46; *see also*, e.g., *id.*, ¶32 (“Based on this CE label, receiving CE 214 identifie[d] the first set of actions.”); Franz, ¶78.)

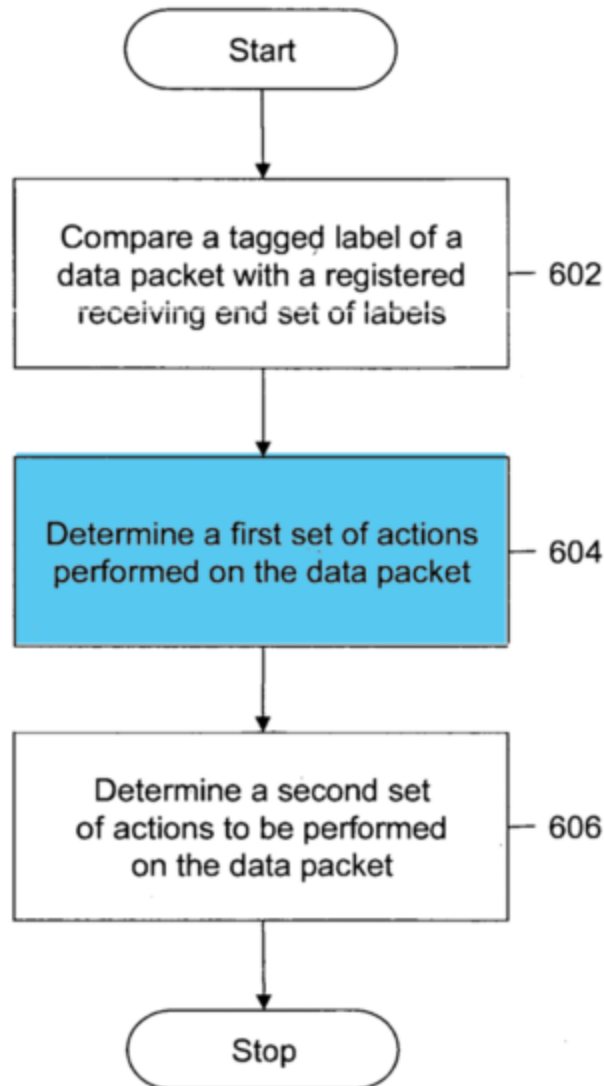


FIG. 6 (Annotated)

Chandra also disclosed that if the data packet was not tagged with a recognized CE label, a third set of actions was performed on the data packet. (Chandra, ¶48; Franz, ¶79.)

- e. **1[d][i]: “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,”**

Chandra disclosed that the receiving CE (first network security appliance) determined the actions it would perform based on the actions performed by the transmitting CE (second network security appliance).

At **step 606** in Figure 6 (below), receiving CE (214) determined the actions to perform on the data packet based on the actions previously performed by transmitting CE (208). (Chandra, ¶46 (“At step 606, the second set of actions that ha[d] to be performed on the data packet at receiving end 204 [was] determined.”); *see also, e.g., id.*, ¶¶32 (“According to the identified first set of actions, receiving CE 214 determine[d] a second set of actions that ha[d] to be performed on the data packet.”), 18.) A POSITA would have found it obvious that because the second set of actions were locally determined and performed by receiving CE (214), they were “local” network security operations. (Franz, ¶82.)

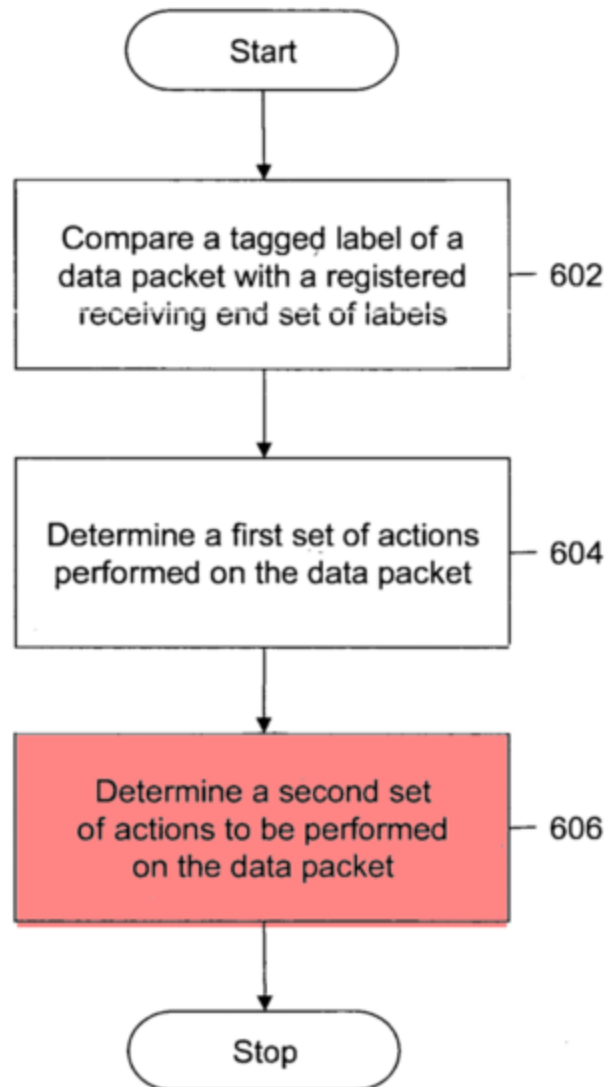


**FIG. 6** (Annotated)

- f. 1[d][ii]: “including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance;”

Chandra disclosed the receiving CE (first network security appliance) not

performing (skipping) the one or more network security operations that were executed by the transmitting CE (second network security appliance). (Chandra, ¶37 (“The second set of actions [to be performed by receiving CE] *includes non-redundant actions that are not present in the first set of actions* [already performed by transmitting CE]. Therefore, *redundant actions are obviated and not performed at receiving CE* [/.”]; Franz, ¶83.)

For example, if receiving CE (214) received a data packet tagged with the CE label “1256” as indicated below, it would determine “that actions corresponding to rules A and B ha[d] been performed on the data packet by transmitting CE 208. Therefore, *receiving CE 214 [could] obviate th[o]se redundant actions.*” (Chandra, ¶53.)

| 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 |
| . . .      |               |                                |

- g. 1[e]: “and executing, by the first network security appliance, the one or more local operations on the network traffic.”

Chandra disclosed that the receiving CE (first network security appliance) executed the second set of actions (one or more local operations) on the data packet (network traffic). (*Id.*, ¶46 (“Once determined, the *second set of actions [was]*

*performed on the data packet at receiving CE [ ].”*; Franz, ¶85.)

2. Claim 2

- a. 2[a]: “The method of claim 1, wherein said determining, by the first network security appliance, one or more network security operations of the first network security appliance 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”

*See* element 1[d][i].

- b. 2[b]: “further comprises determining, by the first network security appliance, one or more network security operations that are to be executed by the first network security appliance except the one or more network security operations that are executed by the second network security appliance based on local network polices [sic].”

Chandra disclosed that receiving CE (first network security appliance) determined one or more actions to perform except the one or more actions that are executed by the transmitting CE (second network security appliance) based on local network polices.

Chandra disclosed that the “[t]he second set of actions [performed by receiving CE] *include[d] non-redundant actions* that [were] not present in the first set of actions [performed by transmitting CE].” (Chandra, ¶37; *see also, e.g.,* ¶¶18, 35.)

Returning to the example in limitation 1[d][ii], receiving CE (214) determined that actions corresponding to rules A and B had been performed by transmitting CE

(208) and skip those actions. (*Id.*, ¶53.) A POSITA would have found it obvious from this disclosure that receiving CE (214) could then perform actions that had not been performed by transmitting CE (214), such as actions corresponding to rule C and/or rule D. (*See, e.g., id.*, ¶35 (“Since the *second set of actions include[d] non-redundant actions*, redundant actions [were] obviated.”); Franz, ¶89.)

| 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 |
| ...        |               |                                |

**“local network policies”**: Although the claim language does not specify whether “based on local network policies” applies to the first network security appliance’s operations, the second network security appliance’s operations, or both, Chandra disclosed this limitation regardless. A POSITA would find it obvious that Chandra contained two sets of local policies: one local to receiving CE and another local to transmitting CE. Each set was stored at and executed by the respective CE. (Franz, ¶90.)

**3. Claim 3**

**a. 3[a]<sup>3</sup>**

*See* element 2[a].

**b. 3[b]: “further comprises determining, by the first network security appliance, that the one or more network security operations that are executed by the second network security appliance are to be executed by the first network security appliance.”**

Chandra disclosed that the receiving CE (first network security appliance) determined one or more actions to perform that are executed by the transmitting CE (second network security appliance).

Chandra disclosed that the second set of actions to be performed at the receiving end could include “nonredundant actions that ha[d] not been performed on the data packet at the transmitting end” and “[could] include redundant actions that ha[d] been performed on the data packet at the transmitting end.” (Chandra, ¶18.) While skipping certain previously-performed actions reduced redundancy, in some circumstances, repeating some actions might be appropriate or more convenient. For example, an upstream device could perform a broad scan, while a downstream device performed a more focused scan that partially overlapped with

---

<sup>3</sup> This limitation repeats another claim limitation. Such repetitions are omitted in this Petition.

the prior one. Consequently, a POSITA would have found it obvious that the actions performed by receiving CE could include both redundant and nonredundant actions. (Franz, ¶93.)

#### 4. Claim 4

- a. **“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.”**

Chandra disclosed that if receiving CE (first network security appliance) received a data packet that was not transmitted from transmitting CE (second network security appliance), receiving CE performed at least one local action specified by a local policy.

Chandra disclosed that when “the data packet ha[d] not been tagged with a CE label or the tagged CE label [was] not recognizable by receiving CE 214...a third set of actions c[ould] be performed on the data packet.” (Chandra, ¶47). It would be obvious to a POSITA that the absence of specific labels associated with the transmitting CE might be indicative of traffic not being transmitted from the transmitting CE, and it would also be obvious that the third set of actions executed by the receiving CE would be one or more local network security operations specified by one or more local policies. (Franz, ¶95.)

In Figure 7 (below), Chandra disclosed that receiving CE determined if a

received data packet had a label that matched the registered set of labels. (Chandra, ¶¶47-48, 53.) If the data packet did not have a recognized label (e.g., the traffic originated from the Internet), receiving CE identified the packet as non-secure and performed a third set of actions on the packet. (*Id.*) Because each CE label used by transmitting CE to tag the data packet was registered at receiving CE, Chandra taught or suggested that when receiving CE checked the data packet at step 702, the presence of a registered CE label in the data packet indicated that the data packet was transmitted from transmitting CE, and an unregistered CE label or an absence of CE label indicated that the data packet was not transmitted from transmitting CE. (Franz, ¶96.)

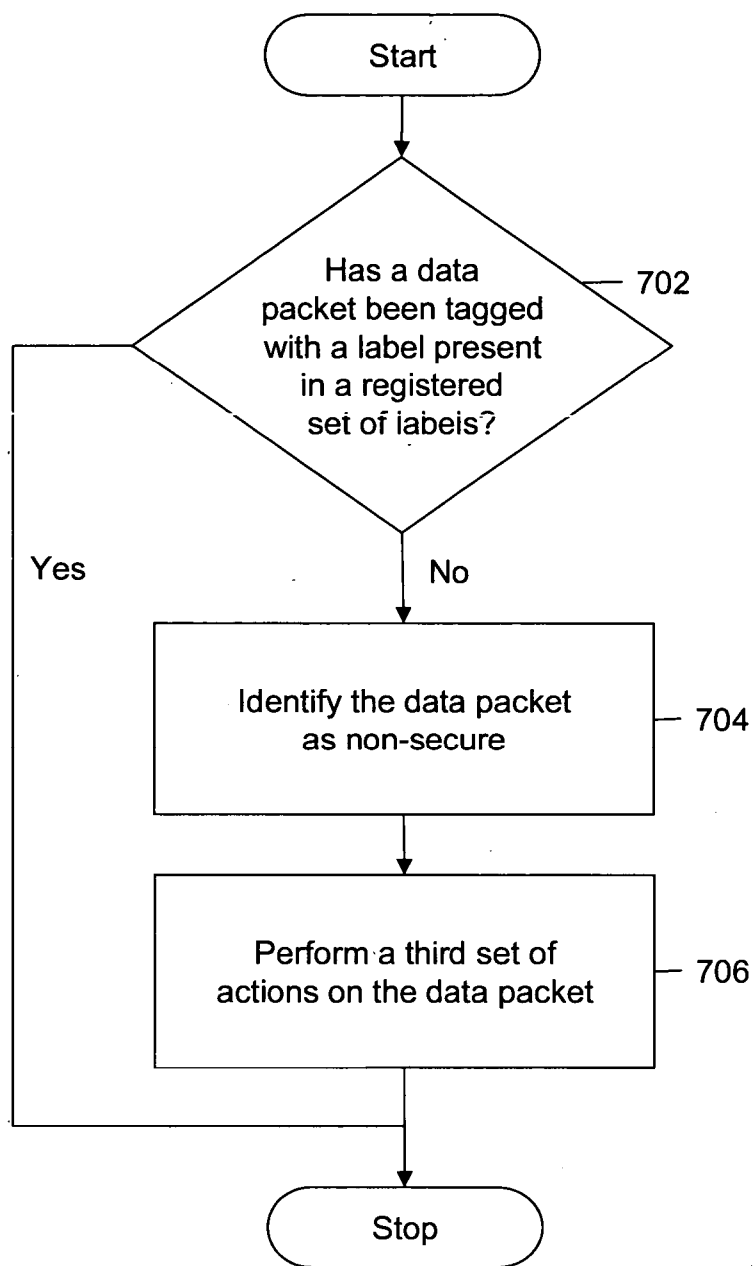


FIG. 7

**5. Claim 5**

- a. “The method of claim 1, wherein the flag indicates the network security operations executed by the second network security appliance.”**

Chandra disclosed that the CE label (flag) indicated the actions executed by transmitting CE (second network security appliance). Specifically, Chandra disclosed that, once transmitting CE (208) performed a first set of actions on a packet, “it tag[ged] the data packet with a CE label *indicating the first set of actions that ha[d] been performed.*” (Chandra, ¶31.)

A POSITA would have found it obvious that Chandra’s “actions” corresponded to “network security operations.”

**6. Claim 12**

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

While Chandra did not expressly disclose that the packets in which the flag was carried comprised a first packet of a session, a POSITA would have found that limitation obvious.

The most commonly used internet protocol, TCP/IP is “connection-oriented”: a connection needs to be explicitly established between a client and a server before data can be sent. There is also a mechanism to explicitly close connections and thereby free up resources. The sequence of interactions between any two communicating parties, starting with the opening of a connection, encompassing any

subsequent data exchange between these parties, and ending with the closing of the connection, is commonly also called a “session.”

It would have been obvious to a POSITA that for the specific objective of communicating a flag or set of flags between a connection initiator and the connection end point of a TCP/IP connection, including 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. They do not, however, necessarily travel along the same route between these end points. A POSITA would have known that if there is just a single route between the two end points of a connection, then all subsequent packets in the connection will travel along the same path, whereas if there are multiple alternative routes, the path may be different while the end points will be identical. Hence, it would have been obvious to a POSITA that for connections without alternative routes, flags in a given session would be redundant after the initial packet. (Franz, ¶¶100-01.)

**7. Claim 15**

**a. 15[pre]-15[d][i]**

*See* limitations 1[pre]-1[d][i].

- b. **15[d][ii]: “including determining one or more network security operations that are to be executed by the first network security appliance except the one or more network security operations that are executed by the second network security appliance based on local network polices;”**

*See* limitation 2[b]. For example, Chandra disclosed that the “[t]he second set of actions [performed by receiving CE] *include[d] non-redundant actions* that [were] not present in the first set of actions [performed by transmitting CE].” (Chandra, ¶37; *see also, e.g.,* ¶¶18, 35.)

- c. **15[e]**

*See* limitation 1[e].

## **8. Claim 16**

*See* claim 5.

## **9. Claim 21**

- a. **21[pre]-21[d][i]**

*See* limitations 1[pre]-1[d][i].

- b. **21[d][ii]: “including determining, by the first network security appliance, that the one or more network security operations that are executed by the second network security appliance are to be executed by the first network security appliance;”**

*See* limitation 3[b]. For example, Chandra disclosed that “the second set of actions [to be performed at the receiving end] *[could] include redundant actions that ha[d] been performed* on the data packet at the transmitting end.” (*Id.*, ¶18;

Franz, ¶107.)

**c. 21[e]**

*See* limitation 1[e].

**10. Claim 22**

*See* claim 5.

**11. Claim 27**

**a. 27[pre]-27[b][i]**

*See* limitations 1[pre]-1[b].

**b. 27[b][ii]: “wherein the flag indicates the network security operations executed by the second network security appliance;”<sup>4</sup>**

*See* claim 5.

**c. 27[c]-27[e]**

*See* limitations 1[c], 1[d][i], and 1[e].

**B. Ground 2: Chandra and Buruganahalli render claims 6-7, 17-18, 23-24, and 28-29 obvious.**

**Buruganahalli:** Much like the ’825 patent, Buruganahalli disclosed a method for network security devices to coordinate security actions. Specifically,

---

<sup>4</sup> “[T]he network security operations” lacks antecedent basis and is assumed to refer to the network security operations that second network security appliance executes before transmitting the packet to the first network security appliance.

Buruganahalli disclosed that, once a network device performed actions on traffic, it used a metadata tag carried by network traffic to indicate the actions performed by the device, thereby eliminating the need to repeat those actions. (*See, e.g.*, Buruganahalli, ¶¶26-30.)

Specifically, Buruganahalli’s Figure 2 (below) depicted network (18) that included various network devices, each of which “may be configured to perform complex processing...on network data [] per packet basis looking for malicious content.” (Buruganahalli, ¶26.) The network devices could be security devices “such as, for example, an intrusion protection system, a data loss prevention system, a fire wall, a load balancer,” etc. (*Id.*, ¶30.)

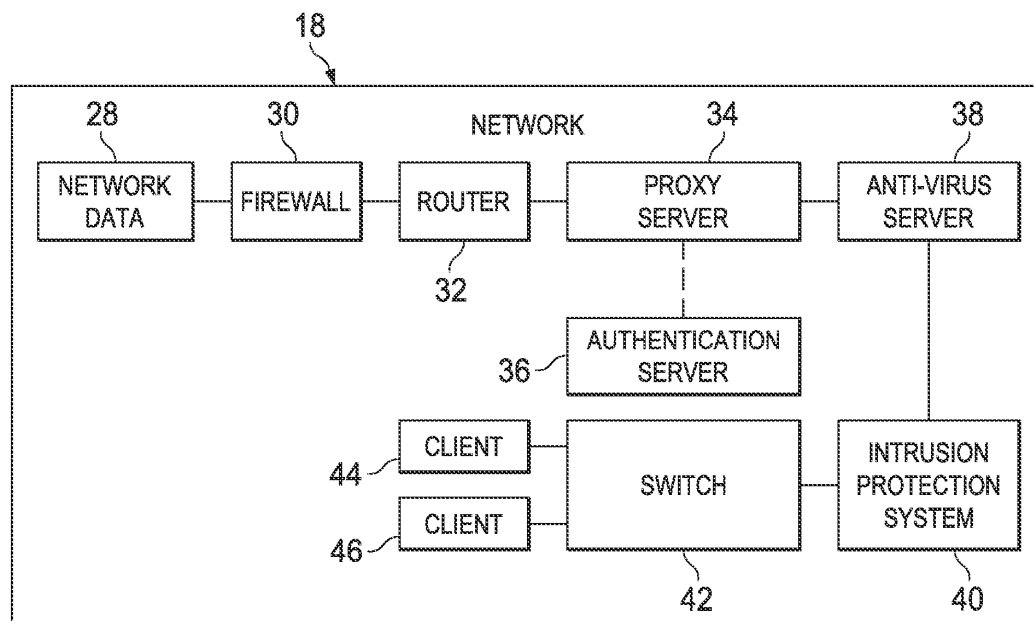
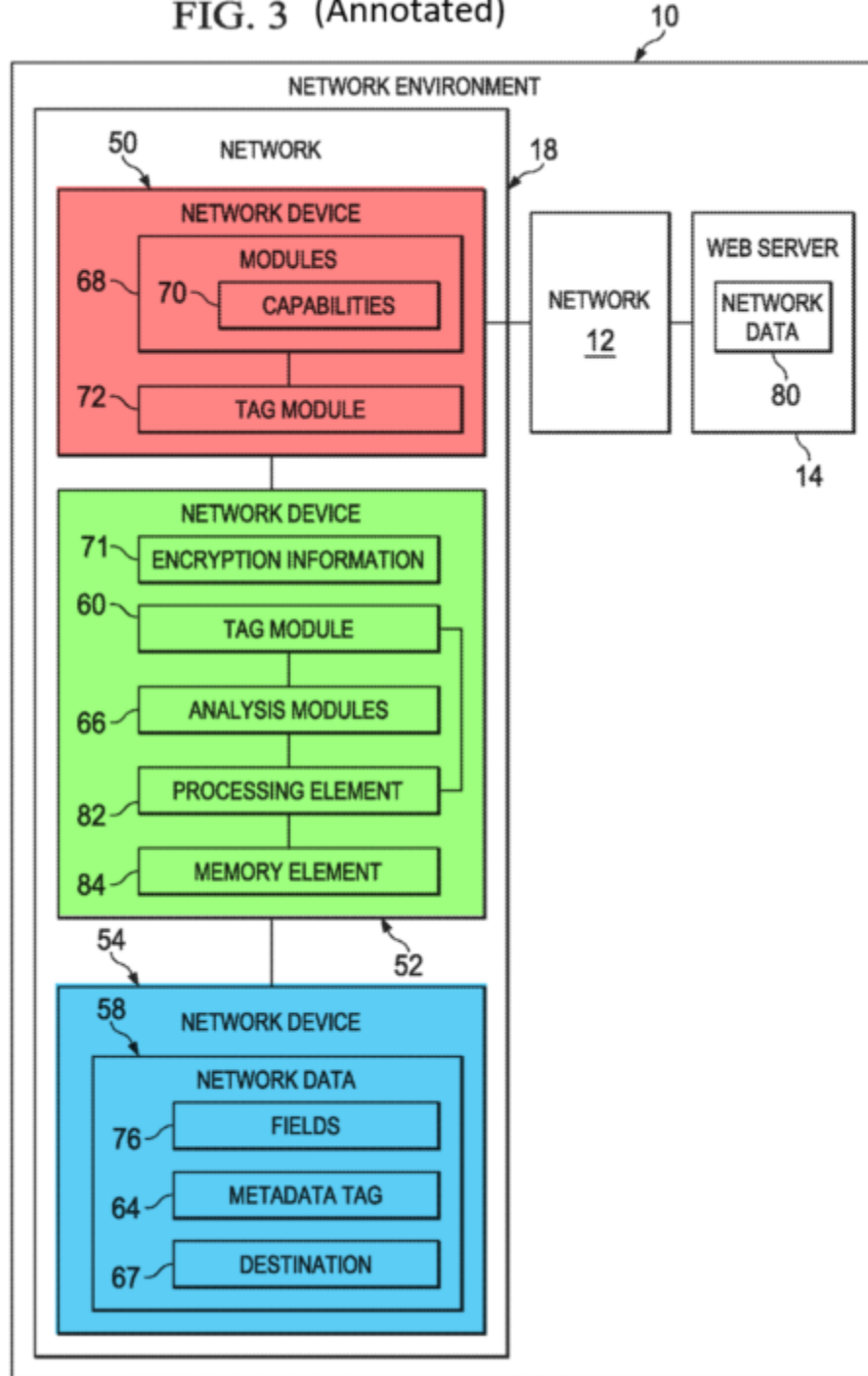


FIG. 2

In operation, the network data carried a metatag tag that included information regarding “processing performed by a previous network device through which network data [] ha[d] already traveled.” (*Id.*, ¶27.) The next network device receiving the network data analyzed the metadata tag to determine what additional processing to perform “without having to repeat actions already performed by the previous network device.” (*Id.*, ¶27; *see also, e.g., id.*, ¶28.) Buruganahalli’s Figure 3 (below) depicted an embodiment that followed this process.

FIG. 3 (Annotated)



Network device (50), network device (52), and network device (54) were connected within network (18). (*Id.*, ¶32.) When network data (58) traveled from network device (54) to network device (52), it carried metadata tag (64) that included

“processing of network data 58 by network device 54.” (*Id.*, ¶36.) For example, the information could include a virus scan result or an intrusion protection scan result. (*Id.*) If the network data included a metadata tag, analysis module 66 then performed a “number of actions based on...metadata tag 64.” (*Id.*, ¶38.) Network device 52 could then “add or update...metadata tag 64” to indicate the processing it performed and send network data (58) to network device (50). (*Id.*, ¶40, 46.)

### **1. Motivation to Combine**

A POSITA would have been motivated to combine Chandra and Buruganahalli with a reasonable expectation of success.

Chandra and Buruganahalli both concerned coordinating network security actions to reduce redundancy. For example, Chandra disclosed network security devices transmitting CE and receiving CE coordinating operations using labels. (Chandra, Abstract, ¶30.) Likewise, Buruganahalli disclosed network devices in a data path coordinating operations using a metadata tag carried by data packets. (Buruganahalli, Abstract, ¶¶27, 28.) Thus, a POSITA looking to improve Chandra would have looked to Buruganahalli’s complementary disclosures.

Additionally, element-specific motivations to combine are discussed below.

### **2. Claims 6, 17, 23, 28**

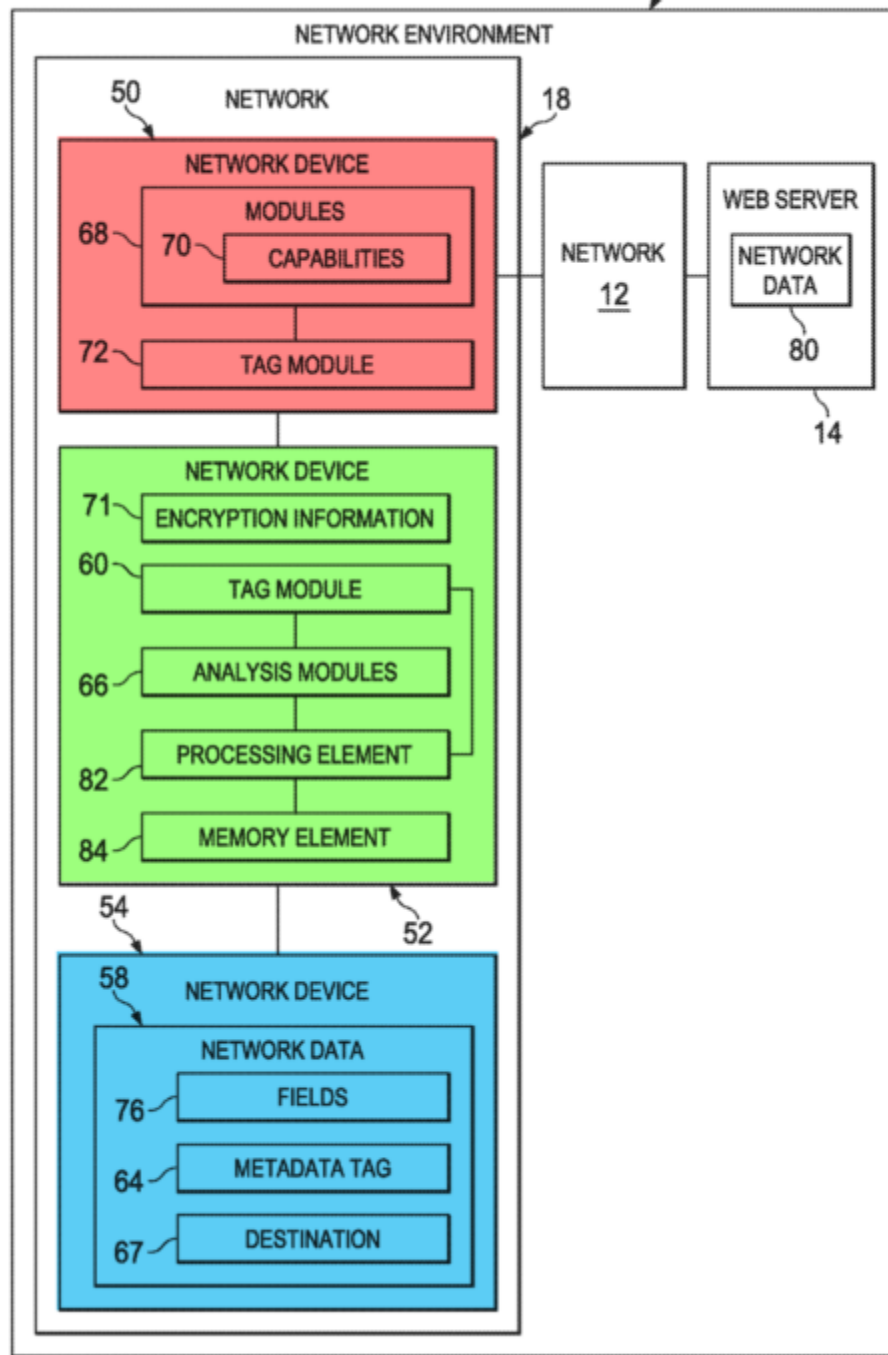
Reciting similar limitations, these claims are analyzed together.

- a. 6[a]/17[a]/23[a]/28[a]: “The method of claim [1/15/21/27], further comprising: updating, by the first network security appliance, the flag to indicate the network security operations executed by the first network security appliance;”

Buruganahalli disclosed that a network device updated a metadata tag (flag) to indicate the operations performed by the network device.

Buruganahalli’s Figure 3 (below) depicted “[n]etwork device 50, network device 52, and network device 54 [] connected within network 18.” (Buruganahalli, ¶32.)

FIG. 3 (Annotated)



First, network device (52) received network data (58) from network device (54). Network data (58) included metadata tag (64). After receiving the data, analysis module (66) performed a “number of actions based on...metadata tag 64” on

network data (58). (*Id.*, ¶38.) Afterwards, tag module (60) “***add[ed] or update[d]*** fields 76 to metadata tag 64 to form metadata tag 64” and “[f]ields 76 may separate the different types of analysis performed on network data 58.” (*Id.*, ¶40.) A POSITA would have found it obvious that Buruganahalli disclosed updating the fields in the metadata tag to indicate the analysis performed on network data by the device that had received the data. (Franz, ¶121.)

A POSITA would have been motivated to add Buruganahalli’s feature of updating the metadata tag to Chandra. If each device added its own label indicating actions it performed to the data packet, that would increase the time it took for the next device to read and process the packet, thereby increasing latency and wasting resources. In addition, the space required to store the labels would keep increasing along the data path. To prevent these issues, a POSITA would be guided by Buruganahalli to update Chandra’s metadata tag, so that each CE along the data path updated the CE label instead of adding a new one. (Franz, ¶122.)

- b. 6[b]/17[b]/23[b]/28[b]: “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.”**

Buruganahalli disclosed network device (52) transmitted the network traffic with the updated flag to network device (50), which was another device participating in the CSF.

Buruganahalli disclosed that “network device 52 [could] be configured to

send network data 58 to network device 50,” which obviously included metadata tag 64. (Buruganahalli, ¶46; *see also, e.g., id.*, ¶¶44, 48.) Network device (50) participated in a CSF because it was coordinating actions with at least network device (52) to reduce redundancies. (*See, e.g., id.*, ¶27.)

In the Chandra-Buruganahalli combination, a POSITA would incorporate Buruganahalli’s tag updating into Chandra’s receiving CE updating a label and transmitting it to the next network appliance in the CSF. A variety of reasons support this addition. For example, Chandra disclosed that “a plurality of such CEs [could] be associated with a single PE.” (Chandra, ¶28.) In this situation, a POSITA would find it obvious that in the multi-CE data path, a receiving CE would benefit from the updated label from the previous CE indicating what actions had already been performed. In another example, receiving CE (214) could transmit the data packet with updated label to receiving network device (212). This would inform receiving network device (212) of the actions performed, allowing receiving network device (212) to know the packet came from an appliance participating in the CSF and/or the operations those appliances performed.

In yet another implementation, receiving CE could transmit the data packet with updated label to a device in an extended VPN network. Specifically, Chandra disclosed a system with a **transmitting end** and a **receiving end**, shown below in both a general configuration (Figure 2) and a VPN configuration (Figure 8). (Chandra,

¶24, 58.)

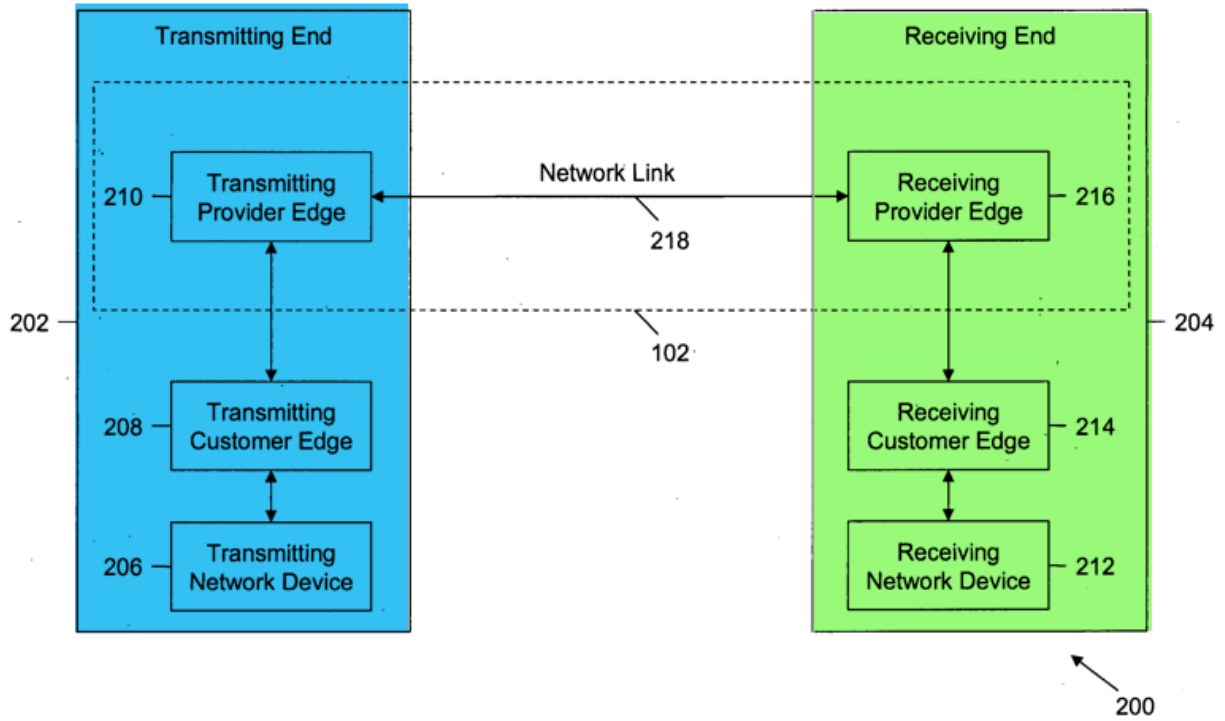


FIG. 2 (Annotated)

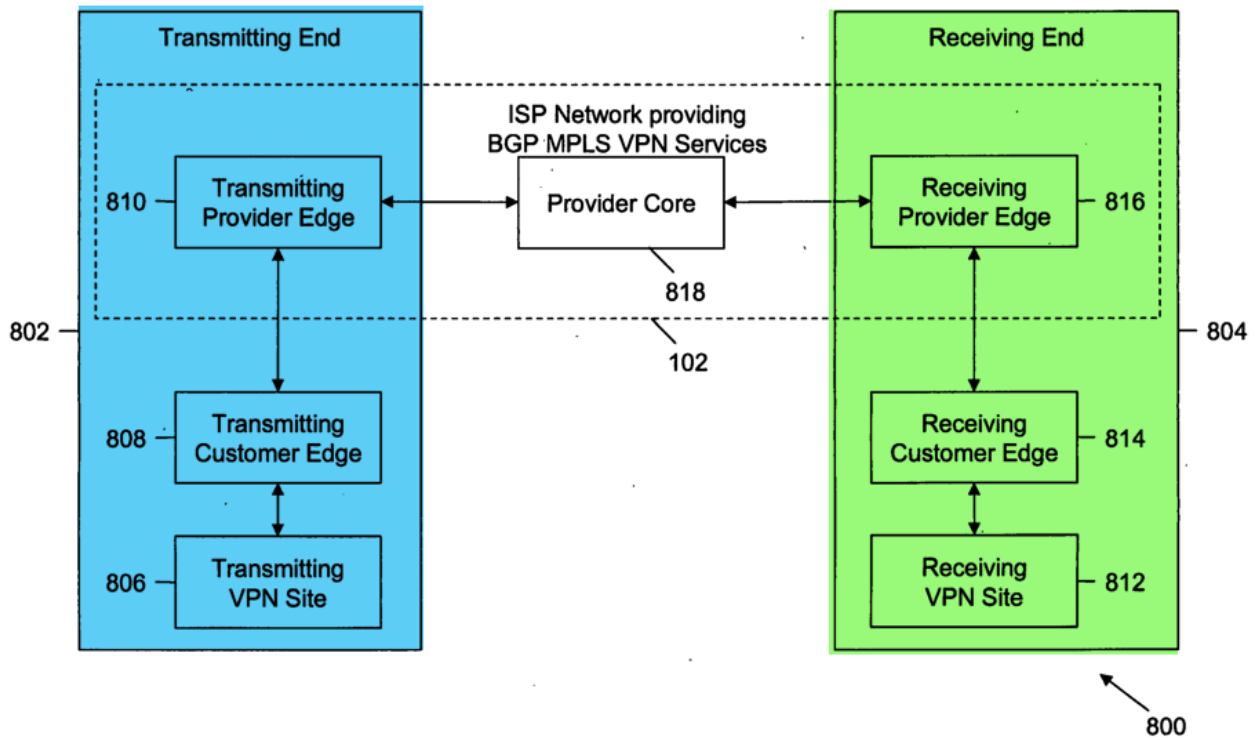


FIG. 8 (Annotated)

Long before the '825 patent, it was well known how to connect one private network (e.g., a remote site of a company) with another (e.g., an enterprise network) using a VPN tunnel. In Chandra, a POSITA would have found it obvious that Figure 8's VPN could be attached as an extension to Figure 2's private network. Figure 2's receiving network device (212) could be coupled with transmitting VPN site (806) and become a gateway that connected the networks in Figures 2 and 8. (See, e.g., Chandra, ¶56; Franz, ¶127-130.) This extended private network is shown in the combined version of Chandra's Figures 2 and 8 (below).

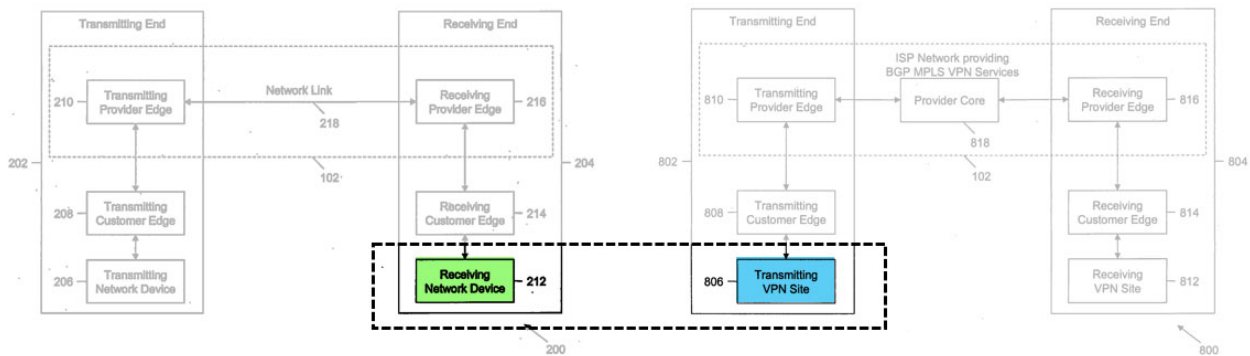


FIG. 2

FIG. 8

(Redrawn and Annotated)

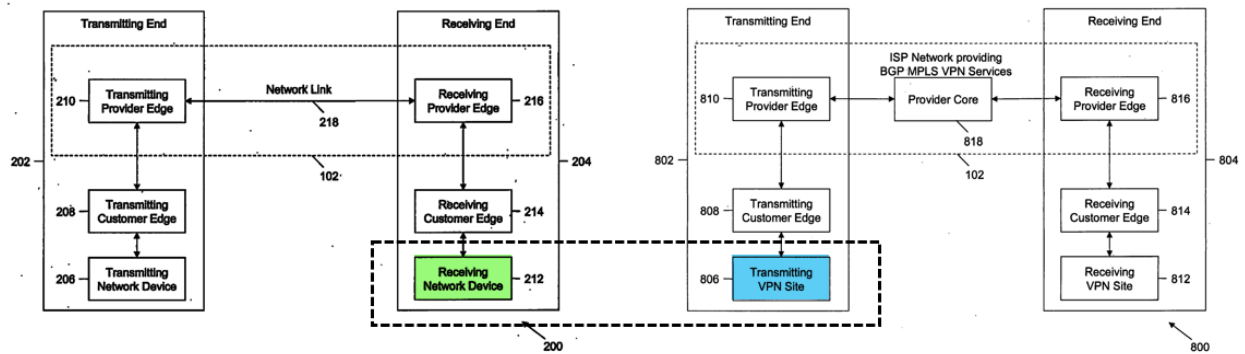


FIG. 2

FIG. 8

(Redrawn and Annotated)

### 3. Claims 7, 18, 24, 29

Reciting similar limitations, these claims are analyzed together.

- a. **“The method of claim [1/15/21/27], 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.”**

Buruganahalli disclosed a network device removing the metadata tag carried by the network data before sending the data to the next device.

Specifically, Buruganahalli disclosed that “last network device to receive the network data prior to sending the data outside of the group of network devices *may remove the metadata tag*. In other embodiments, any network device *may remove the metadata tag*.” (Buruganahalli, ¶29, 47.) In operation, Buruganahalli disclosed that the last network device in the group of devices may remove the metadata tag before transmitting the data to an “undesired network device.” (*Id.*, ¶29.)

Moreover, a POSITA would have been motivated to incorporate Buruganahalli’s teaching to remove a tag from a data packet before passing the packet to another device in Chandra for several reasons. First, removing the tag would keep the network’s labeling mechanism private, preventing malicious devices from intercepting the data packet and exploiting the labeling mechanism. Indeed, Buruganahalli itself recognized this benefit. (*Id.*, ¶29, 47.) Second, removing the tag would prevent compatibility issues in subsequent devices that might not be

compatible with the proprietary tags. (Franz, ¶134.)

**C. Ground 3: Chandra and Kumar render claims 10-11 obvious.**

**Kumar**: Kumar disclosed a method whereby a network node receiving a network packet from another node could authenticate the sending node based on its signature in a security tag within the network packet. (Kumar, Abstract.)

In Figure 1A (below), Kumar disclosed a method in which sending node (20) and receiving node (60) established an authenticated session. (*Id.* ¶¶31, 32.) Using a unique client ID and session key from receiving node (60), sending node (20) created a digital signature. (*Id.* ¶¶33, 36.) Sending node (20) then used the digital signature to create a security tag and inserted it into the outgoing packet, e.g., “in the IP header field.” (*Id.* ¶¶38, 45-46.) Sending node (20) then sent the packet with the security tag to receiving node (60). (*Id.* ¶49.) Receiving node (60) authenticated the security tag by recreating the digital signature and comparing the result against the digital signature contained in the security tag. (*Id.* ¶50.) An authentic security tag indicated that the packet was transmitted from an approved source (sending node (20)), so receiving node (60) accepted the packet and passed it on. (*See id.* ¶55.) Kumar explained that its system could be implemented broadly in the network and could use “any device on [a] network or sub-network that interact[ed] with the stream of packets being secured.” (*Id.*, ¶¶22, 64).

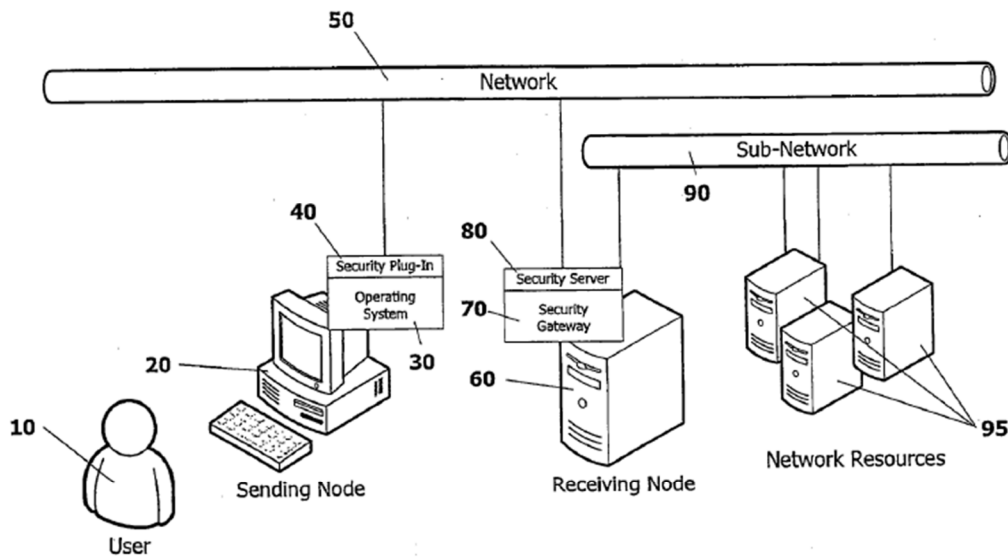


Fig. 1A

## 1. Motivation to Combine

Kumar illustrated the combination of two well-known techniques:

- (1) authenticating another party in a communication using digital signatures, and
- (2) inserting additional information in a data stream that could be decoded by “downstream” devices. Kumar also discussed the traditional technique of inserting such additional information to be communicated “downstream” into packet headers, which has the advantage that no payloads need to be altered. A POSITA would have been motivated to incorporate these techniques into Chandra because they were well-known techniques for securing data packets transmitted between network devices, and were often used predictably and reliably. (Franz, ¶137.)

Additionally, element-specific motivations to combine are discussed below.

## 2. Claim 10

- a. **“The method of claim 1, wherein the flag further comprises or is associated with a signature of the second network security appliance and wherein the method further comprises authenticating, by the first network security appliance, the second network security appliance based on the signature.”**

Although Chandra did not expressly disclose a signature, a POSITA guided by Kumar would find it obvious that Chandra’s method could include a CE label (flag) comprising or being associated with a signature of the transmitting CE (second network security appliance), and the receiving CE (first network security appliance) authenticating the transmitting CE (second network security appliance) based on the signature.

Kumar illustrated the common knowledge that a transmitting device could use information such as client ID, session key, public key, etc., to create a digital signature. (Kumar, ¶36.) The transmitting device could then use the digital signature to create a security tag for insertion into the data packet. (Kumar, ¶¶45-46.) When the data packet reached the receiving device, it could authenticate the security tag using various methods, including recreating the digital signature as discussed above. (*Id.*, ¶49-50; Franz, ¶140.)

A POSITA would have been motivated to incorporate Kumar’s use of digital signatures Chandra. In Chandra’s system, it was important for network security

devices to authenticate the source of the data packet they were receiving to confirm they came from a trusted device and had not been tampered with during transmission. (Chandra, Abstract, ¶30.) Indeed, Chandra disclosed that data packets transmitted from unknown devices would be treated differently from those transmitted from trusted devices. (*See, e.g.*, Chandra, ¶¶47-48, 53.) Thus, because digital signature source authentication was the most popular, practical, and reliable authentication method available, a POSITA wanting to improve Chandra would have looked to incorporate digital signature authentication. (Franz, ¶141.)

In practice, Chandra disclosed that “before transmitting CE 208 and receiving CE 214 c[ould] exchange the CE labels, they ha[d] to authenticate each other.” (Chandra, ¶32.) They could use “an authentication mechanism such as a Message-Digest Algorithm 5 (MD5) based authentication.” (*Id.*, ¶33). A POSITA would find it obvious to take this feature further. Rather than authenticating just at the beginning when the labels are exchanged, the authentication could be applied continuously on every packet exchange using digital signature. (Franz, ¶143.)

### 3. Claim 11

- a. **“The method of claim 1, wherein the flag is carried in an Internet Protocol (IP) header field of the one or more packets.”**

Kumar disclosed the well-known idea that a security tag could be inserted “in the IP header field” of a data packet. (Kumar, ¶38, Franz, ¶144.)

A POSITA would have been motivated to incorporate this well-known technique into Chandra's method. Around the '825 patent's priority date, IP was the most standard and popular network communication protocol. Accordingly, a POSITA would have understood that Chandra's solution, which could be implemented in a VPN environment operating over the public internet, was able to interoperate with IP. An IP data packet was composed of payload and header. A POSITA would have found it obvious that if the IP packet was to carry a label, the header field of the IP packet would be the most natural place to place it; a POSITA would likely not want to modify the payload. Moreover, by allowing for the variable length "options" field in the header, the IP specification itself provides for a natural way to insert such information without jeopardizing compatibility with devices that are unaware of the extension. Therefore, in Chandra's method, a POSITA would have found it obvious to record the CE label in the IP header of the data packets. (Franz, ¶145.)

**D. Ground 4: Chandra and Chandra-2 render claims 13-14, 19-20, 25-26, and 30-31 obvious.**

The claims challenged under this ground merely require that network security devices perform specific, well-known operations. Chandra-2 demonstrated those operations were common knowledge.

A POSITA would find it obvious that Keohane's security elements could perform Chandra-2's operations because each was well-known, commonly

implemented, and would expand Keohane’s range of operations. Because incorporating Chandra-2 into Keohane would merely have involved implementing common elements to yield predictable results, a POSITA would have done so.

#### 4. Claims 13, 19, 25, 30

Reciting similar limitations, these claims are analyzed together.

- a. **“The method of claim [1/15/21/27], wherein the one or more network security operations include network traffic logging.”**

Chandra-2 explained that a “*network security device* c[ould] be a device providing...*logging*.” (Chandra-2, ¶23.) A POSITA would have known network traffic logging is a well-known and widely used network security operation that is especially important for forensic analysis after a vulnerability or breach has been discovered. A POSITA would have found it obvious that “logging” by a network security device might include “network traffic logging.” A POSITA would also have found it obvious that Chandra’s CE, as a network security device, could perform network security logging. (Franz, ¶149.)

#### 5. Claims 14, 20, 26, 31

Reciting similar limitations, these claims are analyzed together.

- a. **“The method of claim [1/15/21/27], wherein the one or more network security operations include one or more of antivirus scanning, intrusion prevention (IPS), content filtering, data leak prevention, antispam, antispyware, reputation-based protections, event correlation, network access control, vulnerability management, load balancing, application control and traffic shaping.”**

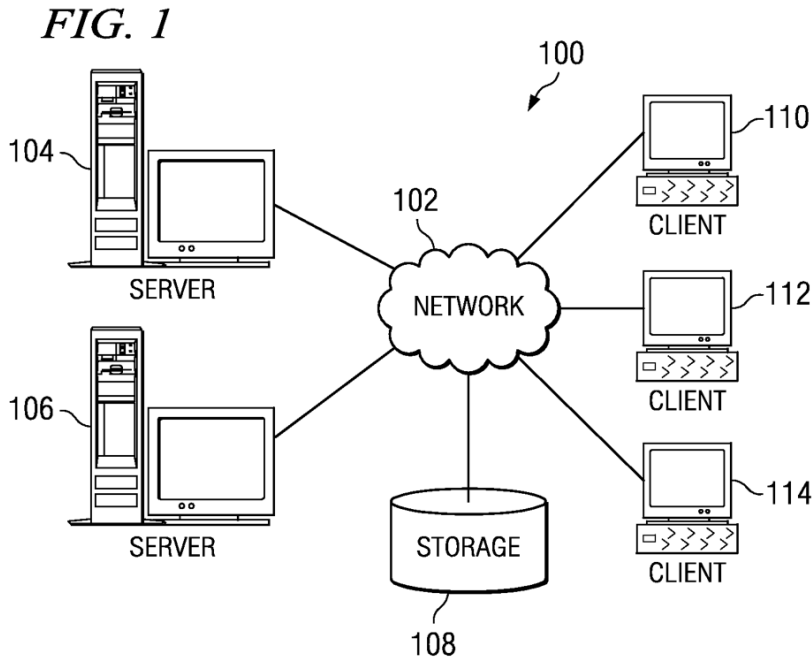
Chandra-2 described that a “network security device c[ould] be a device providing one or more of the following features: *antivirus, intrusion prevention (IPS), content filtering, data leak prevention, antispam, antispyware...reputation-based protections, event correlation, network access control, vulnerability management, load balancing and traffic shaping.*” (Chandra-2, ¶23.) In addition, Chandra-2 described how “functionality that may be provided by a network appliance include[s]...*content filtering.*” (*Id.*, ¶24.) Indeed, the ’825 patent recognizes that DLP and IPS were well-known. (’825 patent, 9:23-26.) A POSITA would have found it obvious that Chandra’s CE could perform any/all of these well-known operations. (Franz, ¶151.)

**E. Ground 5: Keohane renders claims 1-5, 10-12, 15-16, 21-22, and 27 obvious.**

**Keohane:** Similar to Chandra, Keohane was filed over ten years before the ’825 patent and disclosed coordinating operations among security devices to avoid redundant security actions. (Keohane, Abstract, ¶¶9, 10.)

Keohane’s Figure 1 (below) disclosed an embodiment of network data

processing system (100) that included server (104) and server (106) connected to clients (110, 112, and 114) through network (102). (*Id.*, ¶22, 23.)



The clients and servers included “software and/or hardware used to perform security actions.” (*Id.*, ¶23.) Moreover, network (102) included devices to perform security actions, like “routers, gateways, and firewalls.” (*Id.*)

Figure 3 (below) depicted an exemplary multi-level security system. The exemplary system included a data packet (306), firewall (300), mail gateway (302), client (304), and a security database (308). (*Id.*, Fig. 3.)

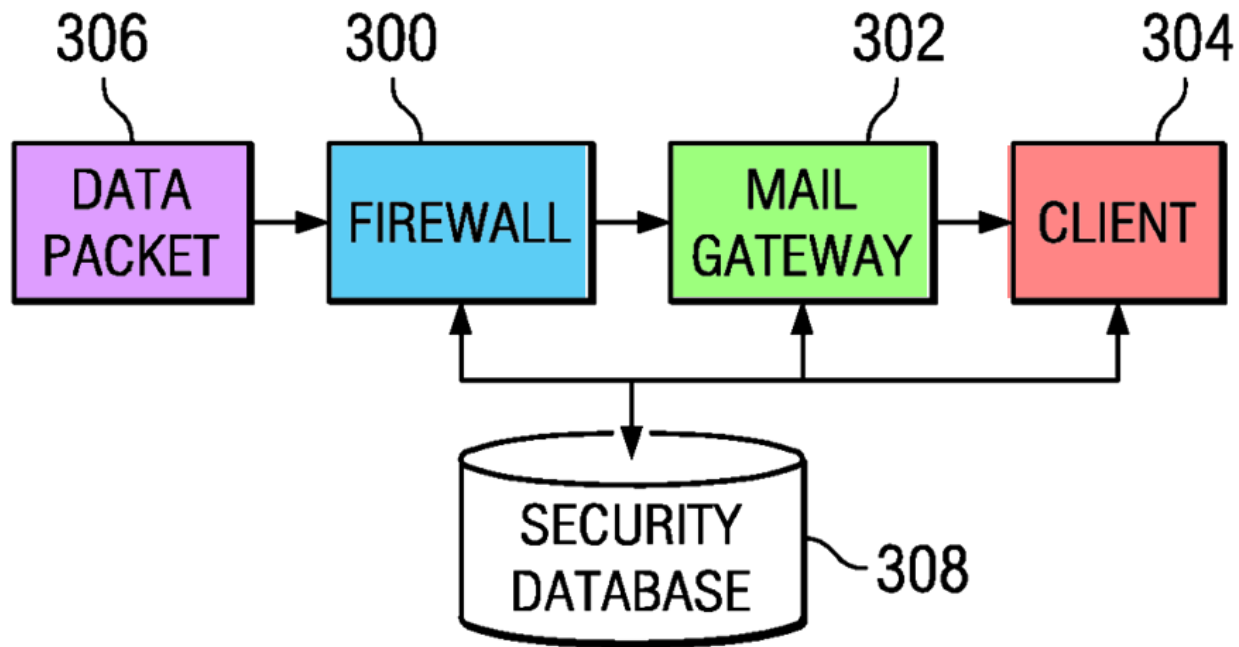
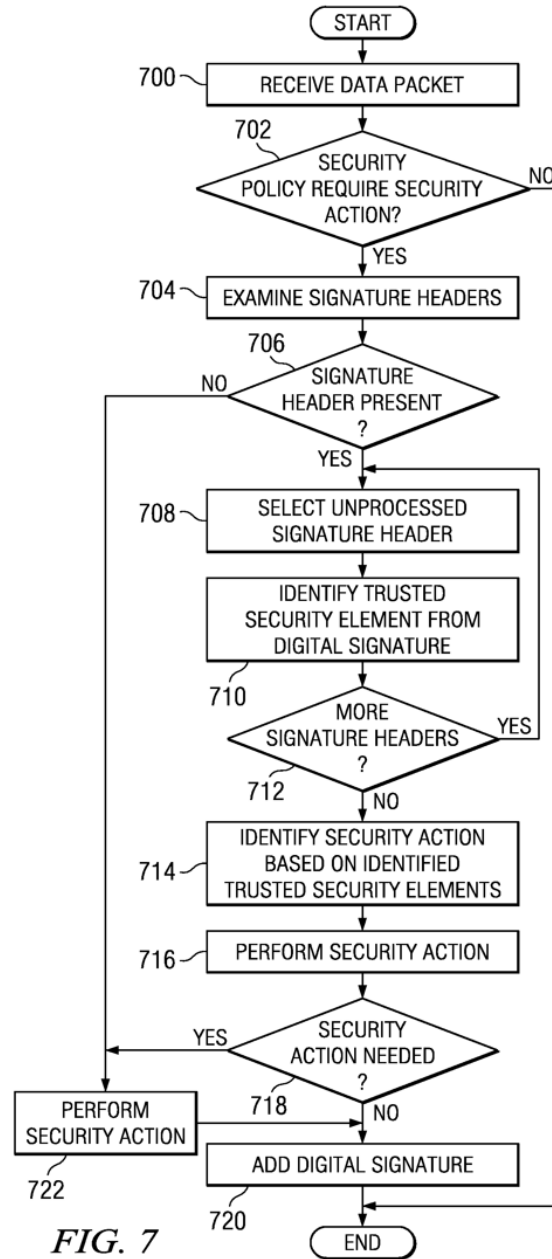


**FIG. 3**  
(Annotated)

The system members cooperated and coordinated with each other to efficiently perform security actions on data packets. In Figure 3’s example, “firewall 300, mail gateway 302, and client 304 form different levels of network security in a network.” (*Id.*, ¶33.) First, firewall (300) received data packet (306), then performed one or more security actions (e.g., determining if packet was from a trusted source) on it. (*Id.*) Afterward, firewall (300) added a digital signature to data packet (306). (*Id.*) The signature was added to the header and “indicate[d] that a security action ha[d] been performed on data packet 306.” (*Id.*, ¶34.) In this example, the signature indicated that firewall (300) determined data packet (306) was from a trusted source. (*Id.*) Firewall (300) then passed data packet (306) to mail gateway (302). (*Id.*, ¶35.)

Once mail gateway (302) received the packet, it examined the header to “determine whether a signature from a trusted security element [was] present in data packet 306.” (*Id.*, ¶35.) In this example, that signature was present, so mail gateway (302) knew firewall (300) had performed that security operation but had not scanned for malware. (*See id.*) Consequently, “mail gateway 302 perform[ed] another security action to scan for viruses and, thereafter, “add[ed] a signature to data packet 306.” (*Id.*, ¶36.) Mail gateway (302) passed the packet to client (304), where the process of determining a security operation from a signature, performing that operation, and adding a signature to the data packet, was repeated. (*Id.*, ¶37.)

Keohane illustrated its method of performing security actions on data packets in Figure 7’s flowchart (below). (*Id.*, ¶52.)



Keohane further disclosed that the security action performed on the data packet could be indicated by inserting a corresponding code into the signature. For example, a code of “01” or “policy 1” could indicate that a trusted source determination had been performed, while “02” or “policy 2” could indicate a virus scan. (*Id.*, ¶38.)

**1. Claim 1**

**a. 1[pre]**

Keohane disclosed a method for screening data packets. (*Id.*, Abstract.)

**b. 1[a]**

Keohane disclosed a firewall (first network security appliance) of a private network (e.g., intranet, LAN, VPN) coordinating security actions with other devices and receiving and inspecting data packets (network traffic).

**“first network security appliance of a private network”**: Keohane disclosed a first network security appliance in the form of **mail gateway (302)** (shown below).

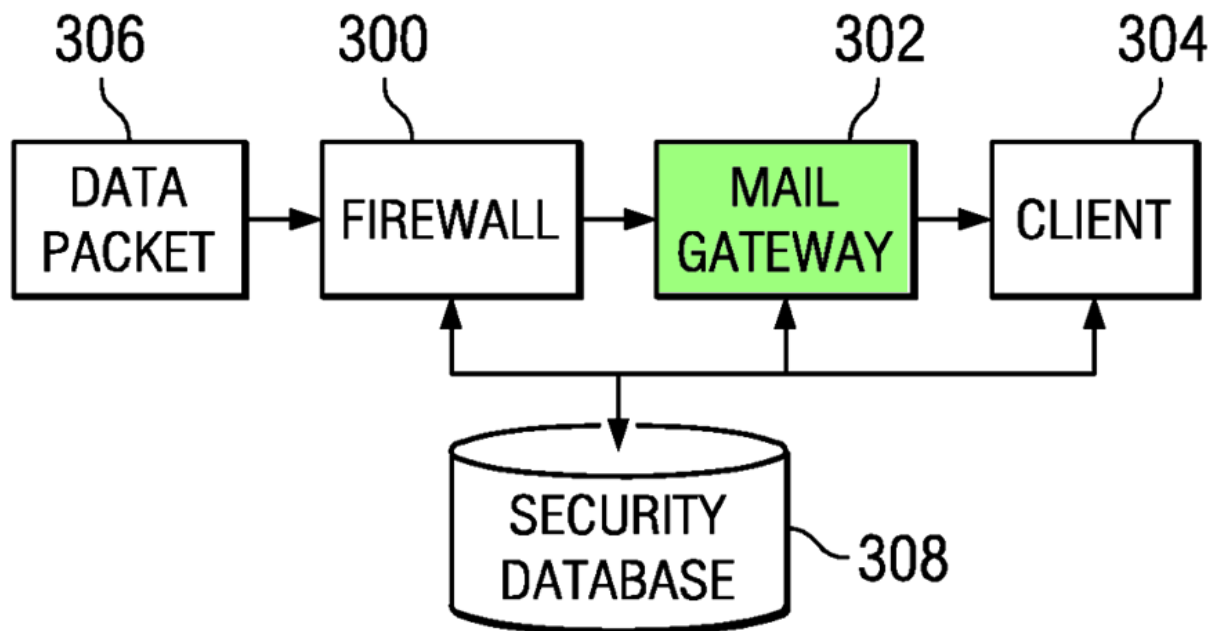
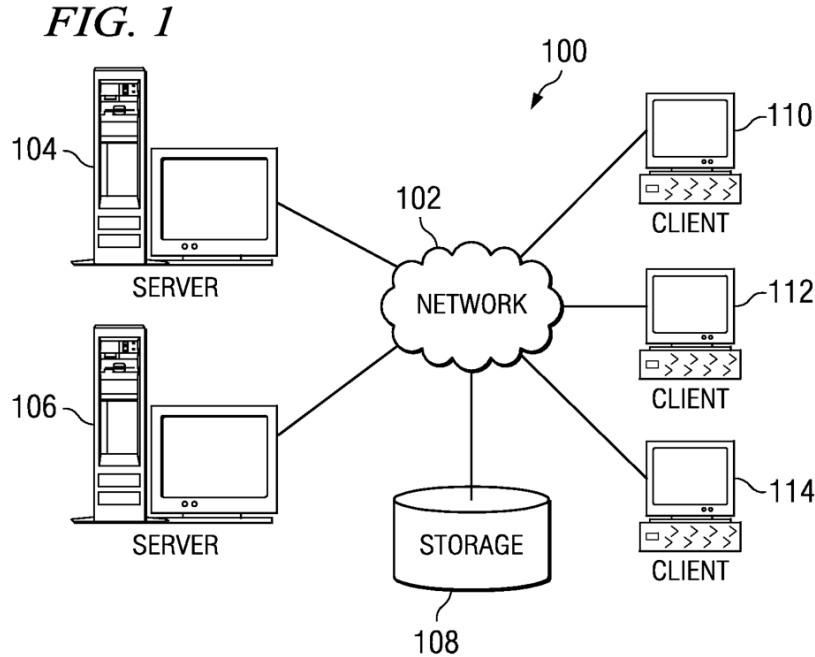


***FIG. 3***  
(Annotated)

(*Id.*, ¶23, FIG. 3.) A POSITA would have found it obvious that the mail gateway constituted a network security appliance because it performed network security

actions (e.g., virus scanning) on traffic. (*Id.*, ¶¶23 (“network 102...includes devices such as...**gateways**...that may...**perform security actions with respect to malware**.”), 36; Franz, ¶160.)

Additionally, Keohane disclosed that mail gateway (302) could be on a private network, e.g., an intranet, LAN, or VPN. (*Id.*, ¶¶24, 32.) Specifically, Keohane disclosed that network (102) (below) provided communications links between various devices in the data processing system and “include[d] devices such as routers, **gateways**, and firewalls that may...perform security actions with respect to malware.” (*Id.*, ¶¶22-23.) This disclosure clearly included mail gateway (302). Keohane also disclosed that network (102) could be an intranet, LAN, or VPN. A POSITA would understand that an intranet was a private network. (*See, e.g.*, Ex. 1009 (“intranet - A private network based on Internet protocols such as TCP/IP but designed for information management within a company or organization.”).) Additionally, as discussed above for Chandra (*see supra*, A1b), a POSITA would have found it obvious that a LAN and VPN were private networks. (Franz, ¶161.)



In addition to mail gateway (302), the first network security appliance could also be any network appliance in the appliance chain (e.g., client (304)) that received network traffic because Figure 3 was not limiting, and a POSITA would understand that the order and number of appliances in Keohane's system could be adjusted. For simplicity's sake, Petitioner focuses its mapping of the first network security appliance on mail gateway (302).

**"participating in a cooperative security fabric (CSF)"**: Keohane disclosed that mail gateway (302) coordinated security actions with other appliances. To do so, each participating appliance inserted a signature into a packet to indicate the security operations performed. (Keohane, ¶11.) Downstream devices determined whether the signature originated from a trusted security element. (*Id.*) If so, the receiving appliance determined the security operations performed by prior devices

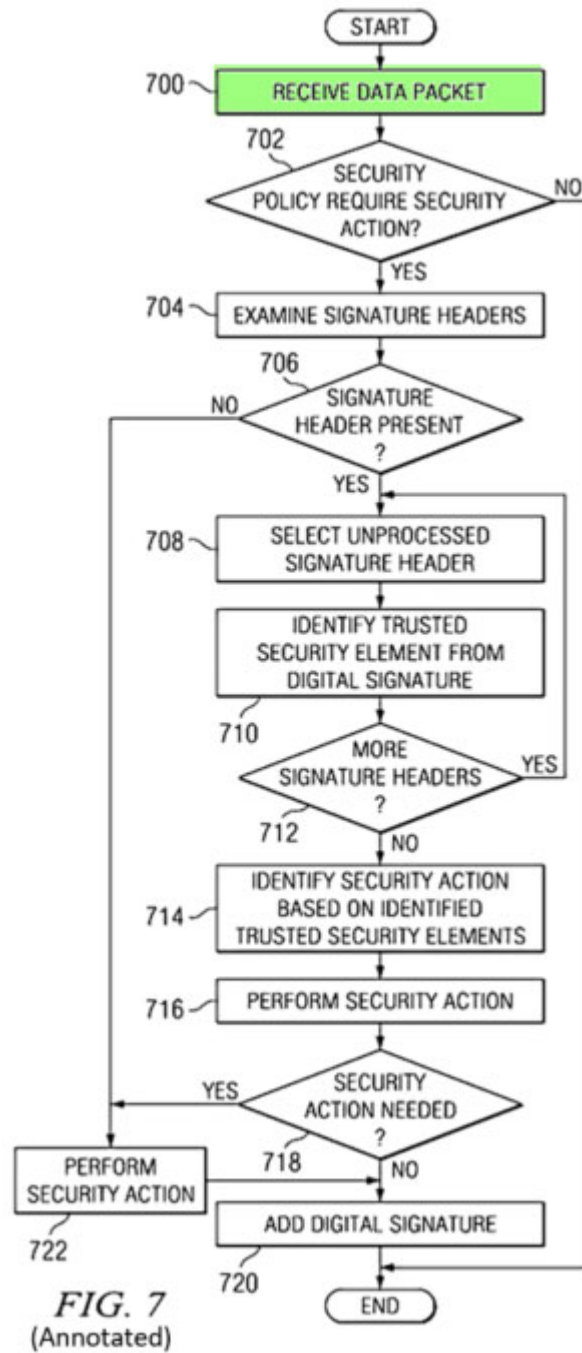
and determined which additional operations to perform. (*Id.*) While not expressly disclosed, a POSITA would have understood that, prior to operation, the appliances participating in Keohane’s system would have been configured to know which code corresponded to which operation. (See, e.g., ¶¶37 (“These *signatures indicate[d]* *that the data packet [was] from a trusted source and that no viruses were found* in data packet 306.”), 38 (“[D]etermination of what security actions have been taken may be *identified by a code in the signature.*”).) Coordinating security actions allowed the system to avoid redundant actions. (Keohane, ¶¶11, 37 (disclosing that “the amount of time and resources used in scanning data packet 306 [was] reduced” and “[u]nneded redundancy [did] not occur, saving time in processing data.”).)

Members of Keohane’s security system performed the same function as the ’825 patent’s CSF, which “coordinates operations among members and avoids redundant operations.” (’825 patent, 5:45-47.) Therefore, a POSITA would have found it obvious that mail gateway (302) participated in a CSF. (Franz, ¶¶163-64.)

*“receiving...network traffic that is to be inspected by the first network security appliance”*: Keohane disclosed that mail gateway (302) received data packet (306) from firewall (300) to inspect it. (Keohane, ¶35.)

Figure 7 (below), for example, depicted a process flow among Keohane’s security elements (e.g., mail gateway). (Keohane, ¶¶35 (“[A] trusted security element [was] a network element, such as a firewall, mail gateway, router, or some

other security intermediary that perform[ed] a security action on a data packet.”),  
52.) At **step 700**, the security element (e.g., mail gateway) “receiv[ed] a data packet.”  
(*Id.*, ¶53.)



Additionally, client (304) received data packet (306) from mail gateway (302)

to inspect it. (*Id.*, ¶37 (“Then, data packet 306 is passed to client 304. Client 304 examines data packet 306.”); Franz, ¶167.)

**c. 1[b]**

Keohane disclosed that mail gateway (302) (first network security appliance) determined whether received packet (network traffic) had been transmitted from another network security element (e.g., firewall (300)) (second network security appliance) based on the packet’s signature (flag).

Keohane disclosed that, after mail gateway (302) received data packet (306) traffic, it “examine[d] data packet 306 to *determine whether a signature from a trusted security element [was] present....*” (Keohane, ¶35; *see also, e.g.*, ¶32 (“When a data packet [was] received, a determination [was] made as to whether a signature of a trusted security element [was] present in the header of the data packet.”).) In [Step 704](#) of Figure 7 (below), for example, Keohane disclosed that a device analyzed the signature in a packet’s header to determine if the packet originated from a trusted security element (e.g., firewall (300)). (*Id.*, ¶54.)

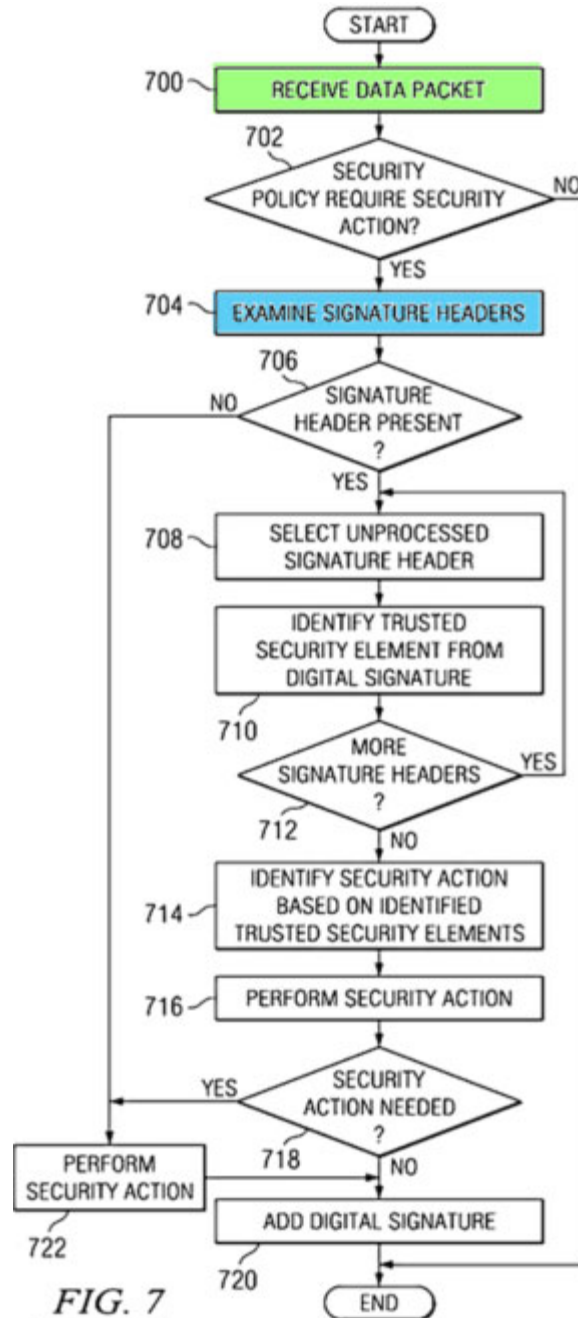


**FIG. 7**  
(Annotated)

Keohane disclosed that the signature in a packet's header was used to determine if the packet had been transmitted from another device in the system. Keohane explained "the signature [was] a digital signature added to the header" of a data packet that could contain a code (e.g., "01" or "02") to indicate what actions

had been taken on a packet. (*Id.*, ¶¶34, 38.) A POSITA would have found it obvious that the digital signature was a flag as described by the '825 patent because the '825 patent broadly described a flag. ('825 patent, 6:28-34 (“flag (e.g., a single bit flag or a collection of bit fields.”).)

Further, a POSITA would have found it obvious that the presence of the signature indicated that the data packet was transmitted from a trusted security element participating in the CSF. This is consistent with the '825 patent's disclosure that a flag's presence in network traffic “indicat[ed] that the network packet [was] transmitted from a member node.” ('825 patent, 6:54-59, 6:65-67.) In addition, a POSITA would have found it obvious that the signature disclosed in Keohane was a well-known authentication method that would be used by the receiving security element to determine if the packet had been transmitted from another trusted security element. Put simply, if the packet header had a signature that the receiving device recognized as being from a trusted security element, the traffic came from another device (second network security appliance) in the CSF. (Franz, ¶171.)

**d. 1[c]**

If a data packet had been transmitted from firewall (300), Keohane disclosed that mail gateway (302) analyzed the signature the packet carried to determine the actions performed on the data packet by firewall (300).

Keohane disclosed that mail gateway (302) checked the signature carried by

data packet (306) from firewall (300) and determined that firewall (300) had performed the security action of determining that data packet (306) was from a trusted source. (*See* Keohane, ¶¶35-36; *see also, id.*, ¶¶37 (“a virus scan...has already been performed by mail gateway 302”), 38.)

Accordingly, Keohane disclosed that “recipients of data packet 306 may identify what security actions ha[d] been performed on data packet 306 to determine what additional security actions [were] to be performed.” (*Id.*, ¶40; Franz, ¶¶173-74.)

**e. 1[d][i]**

Keohane disclosed that mail gateway (302) determined the actions it would perform on a data packet based on the actions performed by firewall (300).

Keohane disclosed that a security element (e.g., mail gateway) performed a security action “selected based on the identified previous security action performed on the data packet [by the previous security element]”. (Keohane, ¶12; *see also, e.g.*, ¶55 (“[A] security action [was] identified based on the identified security elements from the digital signatures (step 714).”), ¶58 (“In response to the signature of the trusted security element being present, a security action [was] then performed in the data packet based on the previous security action.”), ¶32.)

For example, in Figure 3, Keohane disclosed that mail gateway (302) performed a virus scan on data packet (306) because the identified security action

performed by firewall (300) did not include a virus scan. (*See id.*, ¶36 (“Although, firewall 300 allowed data packet 306 to pass, this security element did not perform any scanning for malware. ***As a result, mail gateway 302 perform[d] another security action to scan for viruses.***”).) Similarly, client (204) performed a spyware scan on data packet (306) because the identified security action performed by mail gateway (302) did not include a spyware scan. (*See id.*, ¶37 (“Client 304 scan[ned] data packet 306 for spyware. This security action [was] performed because the other scans did not include scanning data packet 306 for this type of malware. Client 304, however, d[id] not need to perform a virus scan in this example because this type of security action ha[d] already been performed by mail gateway 302.”).) Additionally, Keohane disclosed that “recipients of data packet 306 may identify what security actions have been performed on data packet 306 to determine what additional security actions are to be performed.” (*Id.*, ¶40.)

**f. 1[d][ii]**

Keohane disclosed a security element (e.g., mail gateway) skipping one or more security actions that had already been performed by a previous security element.

For example, in Figure 3, Keohane disclosed that “[c]lient 304...does not need to perform a virus scan...because this type of security action has already been performed by mail gateway 302.” (*Id.*, ¶37.) Keohane also explained that, if mail

gateway (302) had also performed a virus and anti-spyware scan, then “client 304 would taken [sic] no action....” (*Id.*; *see also, e.g., id.*, ¶12 (“The security action may be an absence of an additional action to check the data packet.”).) Finally, Keohane disclosed that a security element could skip all actions depending on the prior actions performed on the data packet. (Keohane, ¶33 (“The security action also may *include taking no action depending on the prior actions taken on a particular data packet.*”).)

**g. 1[e]**

Keohane disclosed that the security element executed the one or more local operations on the data packet (network traffic). (*Id.*, ¶11 (“A *security action [was] performed on the data packet* based on the previous security action performed on the data packet in response to the signature of the trusted security element being present.”), ¶36 (“As a result, mail gateway 302 *perform[ed] another security action to scan for viruses.*”), ¶37 (“Client 304 then *perform[ed] an additional security action* based on the security actions already performed.”); Franz, ¶180.)

**2. Claim 2**

**a. 2[a]**

*See* element 1[d][i].

**b. 2[b]**

Keohane disclosed that mail gateway (302) determined to perform a security operation that had not been executed by firewall (300) based on local policies.

Keohane disclosed that mail gateway (302) determined to perform a virus scan on a data packet but did not determine to perform a trusted source action because firewall (300) had already performed that action. (Keohane, ¶¶34-36.) Specifically, mail gateway determined to perform a virus scan because, “[a]lthough firewall [] allowed data packet [] to pass, [it] did not perform any scanning for malware.” (*Id.*, ¶36.) Consequently, mail gateway “perform[ed] another security action to scan for viruses.” (*Id.*) Thus, mail gateway skipped performing a trusted source action and, instead, performed a malware scan that had not been performed by the firewall.

As another example, Keohane disclosed that client (304) determined the security actions performed by firewall (trusted source analysis) and mail gateway (virus scan). (*Id.*, ¶37 (“These signatures indicate that the data packet [was] from a trusted source and that no viruses were found in data packet 306.”).) Keohane then explained that “[c]lient 304 [] *perform[ed] an additional security action based on the security actions already performed.*” (*Id.*) That action could be a spyware scan because other devices had not performed that action. (*Id.*; *see also, e.g., id.*, ¶40 (“In this manner, other recipients of data packet 306 may identify what security actions ha[d] been performed on data packet 306 to determine what additional security actions [were] to be performed.”).)

**“local network policies”**: Although the claim language is unclear whether the “based on local network policies” limitation applies to the first network security

appliance's operations, the second network security appliance's operations, or both, Keohane disclosed this limitation regardless. A POSITA would find it obvious that in Keohane, there were two sets of local policies: one set local to receiving security element and a second set local to transmitting security element. Each set was stored at and executed by the respective security element.

Keohane disclosed that each element in the system determined the local action(s) it would perform using local network policies. For example, a code of "policy 1" indicated that a trusted source determination had been performed, while "policy 2" indicated a virus scan had been performed. (*Id.*, ¶38.) The codes could be stored locally on each device. (*Id.*)

Similarly, Keohane disclosed that, once a device received traffic, "[a] determination [was] made as to ***whether a security policy requires a security action.***" (*Id.*, ¶53.) The security policy was "a set of rules used to determine what security action to take." (*Id.*) Keohane explained that "[t]he ***security policy [could] be local*** to the component executing the process." (*Id.*) A POSITA would find it obvious that these locally-stored codes and security policies were local network policies instructing the member elements on what security actions to perform or not perform. (Franz, ¶¶185-87.)

**3. Claim 3**

**a. 3[a]**

*See* element 2[a].

**b. 3[b]**

Keohane disclosed that mail gateway (302) determined to perform at least one security operation that had been executed by firewall (300) and skipping the remaining operations.

Keohane disclosed that the security operation performed by the downstream security appliance (e.g., mail gateway (302)) “include[d] *performing another scan on the data packet*, a different type of scan, or no action at all.” (Keohane, ¶32.) Thus, Keohane at least suggested that the network security element could simply perform another scan on the packet rather than a different type of scan or no action at all.

To the extent Keohane did not expressly disclose this limitation, a POSITA would have found it obvious. While skipping certain previously-performed actions reduced redundancy, in some circumstances, repeating some actions might be appropriate or more convenient. For example, an upstream device could perform a broad scan, while a downstream device performed a more focused scan that partially overlapped with the prior one. Consequently, a POSITA would have found it obvious that the actions performed by the receiving device could include both redundant and nonredundant actions. (Franz, ¶191.)

Alternatively, Keohane disclosed that the security operation performed by the security element “include[d] *performing another scan* on the data packet [or] *a different type of scan*.” (Keohane, ¶32.) This suggested that (1) a scan of the same type as a previously-performed scan could be performed, while (2) other scans that had already been performed were skipped and a different type of scan was performed instead. (Franz, ¶192.)

#### 4. Claim 4

Keohane disclosed that if a security element received a data packet that lacked a signature header, certain security actions were performed on the packet.

In Step 706 (below), Keohane disclosed that a determination was made as to whether a signature header was present in a packet. (Keohane, ¶56.) If not, the process proceeded to **Step 722**, which was to perform a security action.

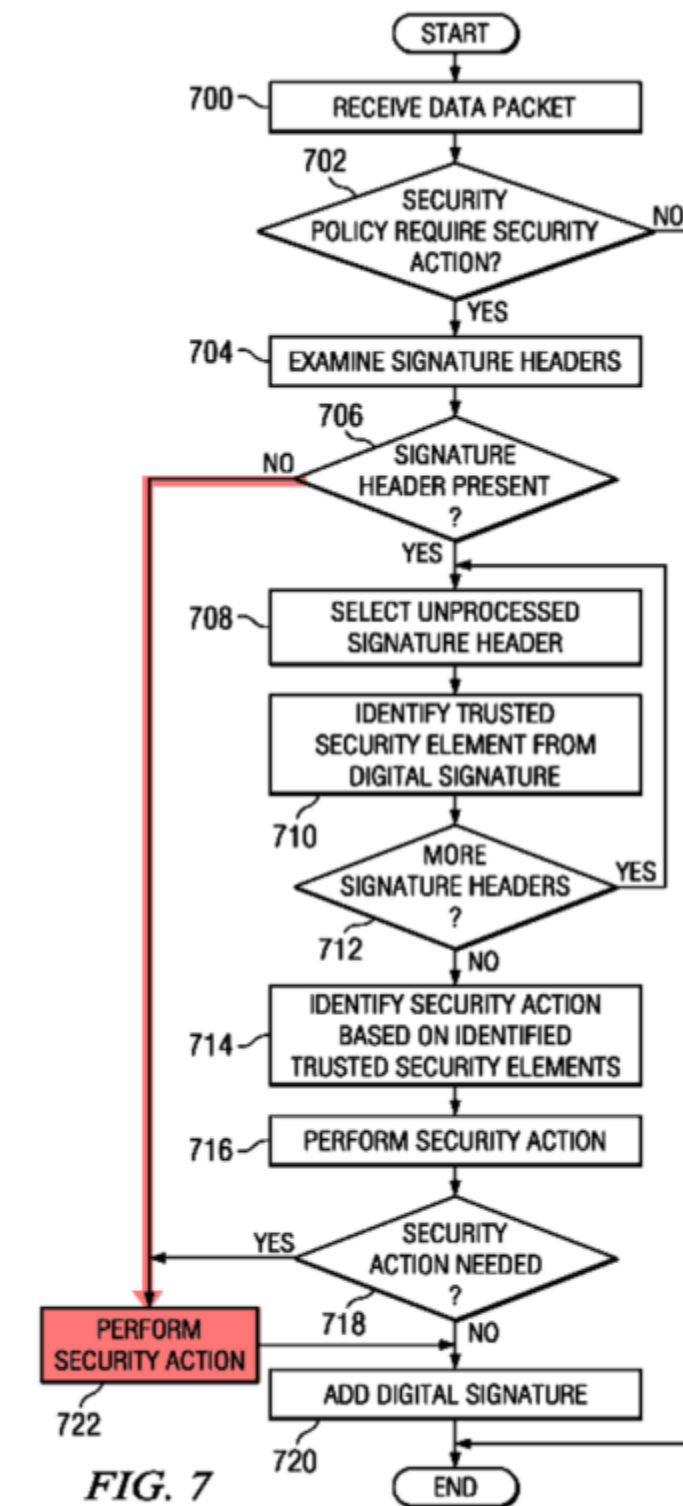


**FIG. 7**  
(Annotated)

A POSITA would have found it obvious that if the packet did not have a signature, it had not been transmitted by an upstream device (second network security appliance) participating in the cooperative security network because Keohane disclosed that each device added a signature to the packet post processing. (*See, e.g., id.*, ¶32.) Thus, a packet without a signature could not have come from upstream.

Additionally, policies specifying security action would be local because Keohane disclosed that a “security policy may be local to the component executing the process.” (*Id.*, ¶53.) Moreover, the security element’s actions would be local operations because they were being performed by the local device that received the traffic and would be executing the actions specified in the local policy. While Keohane did not expressly identify what local actions applied in this scenario, a POSITA would have found it obvious that they could include dropping the packet or performing one or more security actions on it. (Franz, ¶¶196.)

## **5. Claim 5**

Keohane disclosed that the “signature indicate[d] that a previous security action ha[d] been performed [by a previous security element] on the data packet.” (Keohane, ¶32.) For example, Keohane disclosed that firewall (300) added a signature to data packet 306 that “indicate[d] that a security action ha[d] been performed on data packet 306 [by firewall 300].” (*Id.*, ¶34; *see also, e.g.,* ¶¶36-37

(explaining that mail gateway (302) added a signature to the data packet indicating that a security action had been performed on the data packet).) Keohane explained that the security actions could be identified by a code in the signature. For example, a code of “01” could indicate that the data packet’s source was a trusted one, while a “02” code could indicate a virus scan had been performed. (*Id.*, ¶38; Franz, ¶197.)

## 6. Claim 10

Keohane disclosed that a flag in a packet included a signature of a security element (e.g., firewall) and that later security elements receiving the packet used the signature to know if the packet came from a trusted source.

Keohane disclosed that, after a security element performed an action, the security element added a signature to the data packet. (Keohane, ¶34 (“Before passing data packet 306 to mail gateway 302, firewall 300 add[ed] a signature to data packet 306.”).) Keohane explained that the signature was a digital signature added to the header and indicated that a security action had been performed on the packet. (*Id.*) When a downstream device received a packet, it analyzed the signature header to identify what actions had been performed. (*Id.*, ¶54.)

Additionally, Keohane disclosed that, after a security element received a data packet, it “examine[d] data packet [] to *determine whether a signature from a trusted security element [was] present....*” (Keohane, ¶35; *see also, e.g.*, ¶32 (“When a data packet [was] received, a determination [was] made as to whether a

signature of a trusted security element [was] present in the header of the data packet.”.) A POSITA would find it obvious that determining whether the signature was from a trusted security element included authenticating the signature and its source. A POSITA would also find it obvious that the signature disclosed in Keohane was a well-known authentication method to determine if the packet had been transmitted from another trusted device. Put simply, if the packet header contained a signature the receiving device recognized as being from a trusted security element, the traffic came from another device (second network security appliance) inside the CSF. (Franz, ¶200.)

#### **7. Claim 11**

Keohane disclosed the signature (flag) being carried in an IP header field of the one or more packets. Keohane taught that the disclosed method “may be implemented in a data packet using Internet protocol version 6 (IPv6)...In this type of protocol, data packets include[d] a multi-header chain followed by the payload.” (Keohane, ¶40.) Keohane further disclosed that “the signature [was] located in a header of the data packet.” (*Id.*, ¶12.)

#### **8. Claim 12**

While Keohane did not expressly disclose that the packets carrying the flag comprised a first packet of a session, a POSITA would have found that limitation obvious based on knowledge of a POSITA.

As discussed above, a POSITA would have known that TCP/IP includes a sequence of interactions that is commonly called a “session.” (*See, supra*, §VIII.A.6.)

Also as discussed above, a POSITA would have found it obvious that including a flag in the first packet of a session with only one route between endpoints would be sufficient. A POSITA would have known that if there is just a single route between the two end points of a connection, then all subsequent packets in the connection will travel along the same path as the first packet of the session. Hence, for connections without alternative routes, the flags would actually be redundant in packets in a session after the initial packet. (Franz, ¶203-04.)

**9. Claim 15**

**a. 15[pre]-15[d][i]**

*See* limitations 1[pre]-1[d][i].

**b. 15[d][ii]**

*See* limitation 2[b]. For example, Keohane disclosed that mail gateway (302) determined to perform a virus scan on a data packet but did not perform a trusted source action because firewall (300) had already performed that action. (Keohane, ¶¶34-36.) As another example, Keohane disclosed that client (304) determined the security actions performed by firewall (trusted source analysis) and mail gateway (virus scan). (*Id.*, ¶37.) Keohane then explained that “[c]lient 304 [] *perform[ed]* *an additional security action based on the security actions already performed.*” (*Id.*) That action could be a spyware scan because other devices had not performed

that action. (*Id.*; *see also, e.g., id.*, ¶40.)

**c. 15[e]**

*See* limitation 1[e].

**10. Claim 16**

*See* claim 5.

**11. Claim 21**

**a. 21[pre]-21[d][i]**

*See* limitations 1[pre]-1[d][i].

**b. 21[d][ii]**

As discussed in limitation 3[b], Keohane disclosed—or at least suggested—that mail gateway (302) determined to perform at least one security operation that had been executed by firewall (300) and skipping the remaining operations. (Franz, ¶210.)

**c. 21[e]**

*See* limitation 1[e].

**12. Claim 22**

*See* claim 5.

**13. Claim 27**

**a. 27[pre]-27[b][i]**

*See* limitations 1[pre]-1[b].

- b. 27[b][ii]: “wherein the flag indicates the network security operations executed by the second network security appliance;”<sup>5</sup>

*See* claim 5.

- c. 27[c]-27[e]

*See* limitations 1[c], 1[d][i], and 1[e].

**F. Ground 6: Keohane and Buruganahalli render claims 6-7, 17-18, 23-24, and 28-29 obvious.**

**1. Motivation to combine**

A POSITA would have been motivated to combine Keohane and Buruganahalli with a reasonable expectation of success.

Keohane and Buruganahalli both concerned coordinating network security actions to reduce redundant actions. For example, Keohane disclosed coordinating operations among security elements along a data path using signatures to avoid redundant security actions. (Keohane, Abstract, ¶¶9, 10.) Likewise, Buruganahalli disclosed network devices in a data path coordinating operations using a metadata tag carried by data packets. (Buruganahalli, Abstract, ¶¶27, 28.) Thus, a POSITA

---

<sup>5</sup> “[T]he network security operations” lacks antecedent basis and is assumed to refer to the network security operations that the second network security appliance executes on the data packet before transmitting it to the first network security appliance.

looking to improve Keohane would have looked to Buruganahalli's complementary disclosures.

Additionally, element-specific motivations to combine are discussed below.

## **2. Claims 6, 17, 23, 28**

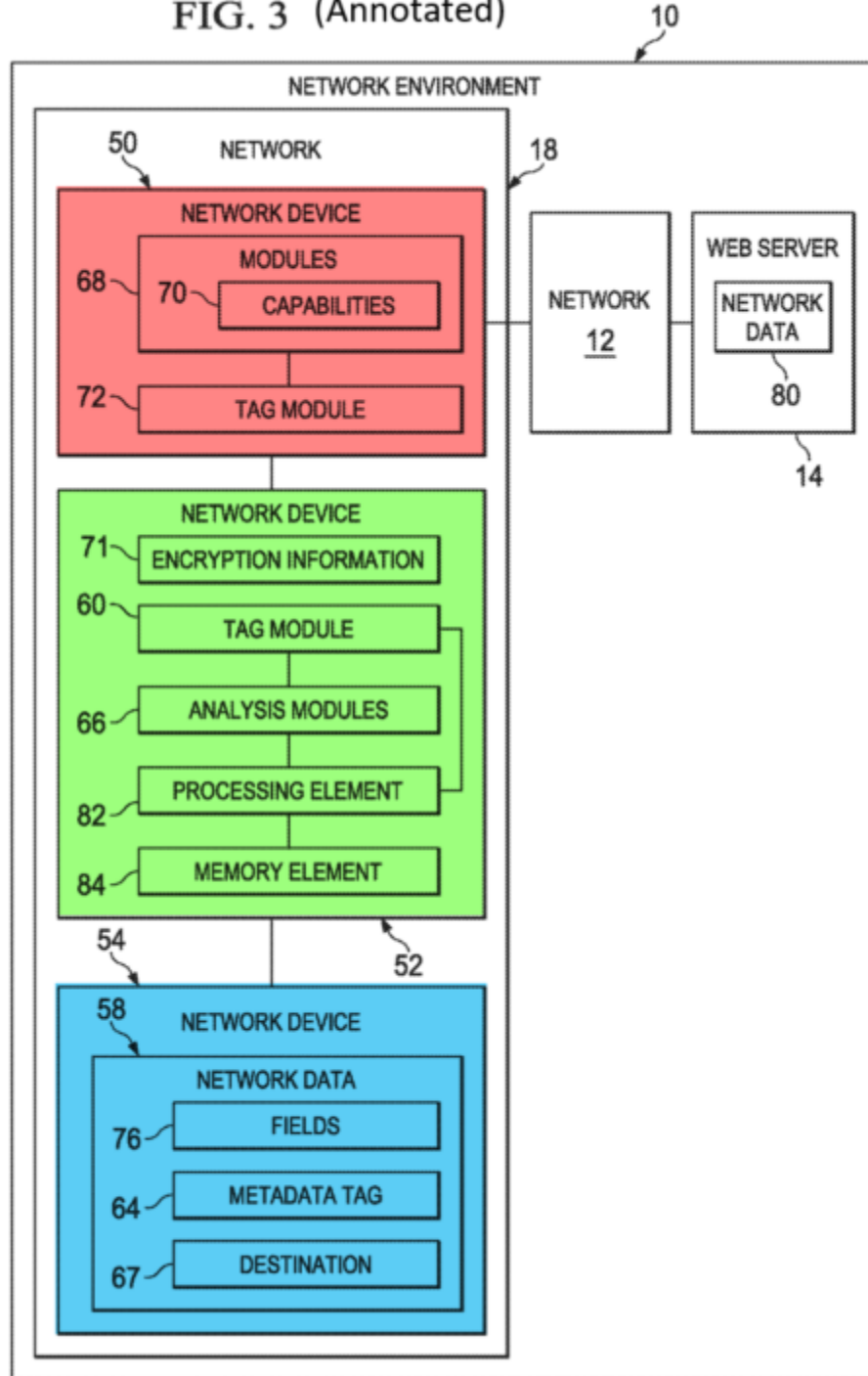
Reciting similar limitations, these claims are analyzed together.

### **a. 6[a]/17[a]/23[a]/28[a]**

Buruganahalli disclosed that a network device updated a metadata tag (flag) to indicate the operations performed by the network device.

Figure 3 (below) depicted “[n]etwork device 50, network device 52, and network device 54 [] connected within network 18.” (Buruganahalli, ¶32.)

FIG. 3 (Annotated)



First, network device (52) received network data (58) from network device (54). Network data (58) included metadata tag (64). After receiving the data, analysis module (66) performed a “number of actions based on...metadata tag 64”

on network data (58). (*Id.*, ¶38.) Afterwards, tag module (60) “*add[ed] or update[d]* fields 76 to metadata tag 64 to form metadata tag 64” and “[f]ields 76 may separate the different types of analysis performed on network data 58.” (*Id.*, ¶40.) A POSITA would have found it obvious that these disclosures included updating the fields in the metadata tag to indicate analysis performed on network data by the device that had received the data. (Franz, ¶222.)

A POSITA would have been motivated to add Buruganahalli’s feature of updating the metadata tag to Keohane. If each security element added its own signature indicating the actions it performed to the data packet, that would increase the time it took for the next element to read and process the actions performed by the prior elements, increasing latency and wasting resources. In addition, the size requirement for storing all the signatures would increase along the data path. To prevent these issues, a POSITA would be guided by Buruganahalli’s teaching regarding updating the metadata tag to use in Keohane, so that each security element along the data path updated the signature before passing the data packet to the next element instead of adding a new signature. (Franz, ¶223.)

**b. 6[b]/17[b]/23[b]/28[b]**

Buruganahalli disclosed network device (52) transmitted the network traffic with the updated flag to network device (50), which was another device participating in the CSF.

Buruganahalli disclosed that “network device 52 [could] be configured to send network data 58 to network device 50,” which obviously included metadata tag 64. (Buruganahalli, ¶46; *see also, e.g., id.*, ¶¶44, 48.) Network device (50) participated in a CSF because it was coordinating actions with at least network device (52) to reduce redundancies. (*See, e.g., id.*, ¶27.)

In the Keohane-Buruganahalli combination, a POSITA would incorporate Buruganahalli’s disclosure of updating a tag into Keohane’s security element updating the signature and transmitting the updated signature to the next security element along the data path. (Franz, ¶226.)

### 3. Claims 7, 18, 24, 29

Reciting similar limitations, these claims are analyzed together.

Buruganahalli disclosed a network device removing the metadata tag carried by the network data before sending the data to the next device. Specifically, Buruganahalli disclosed that “last network device to receive the network data prior to sending the data outside of the group of network devices *may remove the metadata tag*. In other embodiments, any network device *may remove the metadata tag*.” (Buruganahalli, ¶29; *see also, e.g., id.*, ¶47.) In operation, Buruganahalli disclosed that the last network device in the group of devices may remove the metadata tag before transmitting the data to an “undesired network device.” (*Id.*, ¶29.)

Moreover, a POSITA would have been motivated to incorporate Buruganahalli's teaching to remove a tag from a tagged data packet before passing the data packet to another device into Keohane for several reasons. First, removing the tag before passing the data packet would keep the network's labeling mechanism private, preventing malicious devices from intercepting the data packet and exploiting the labeling mechanism. Indeed, Buruganahalli recognized this benefit itself, remarking that the tag could be removed before the packet went to "undesired network devices." (*Id.*, ¶29; *see also, e.g., id.*, ¶47.)

Second, as Keohane suggested, removing the tag would prevent compatibility issues in subsequent devices that might not be compatible with the proprietary tags. Keohane disclosed that in some embodiments, the packet header in which the signature was stored was "a new type of extension header." (Keohane, ¶48.) Keohane's mail gateway (302) could determine that such a header was not compatible with client (304) that only used standard header format. Therefore, mail gateway (302) could remove the signature from the data packet before transmitting the untagged packet to client (304). This provided a motivation to incorporate Buruganahalli, which disclosed removing the metadata tag when the next destination was not within the network's predefined set of destinations, such as when the next destination was not one of the network devices that could read and utilize the tag to cooperate network operations. (*See id.*, ¶¶46-47; Franz, ¶231.)

For these reasons, a POSITA would be guided by Buruganahalli's teaching regarding removing the metadata tag to use in Keohane, so that a security element on the network data path could remove the signature before passing the data packet to the next device.

**G. Ground 7: Keohane and Kumar render claims 10 obvious.**

**1. Motivation to Combine**

Kumar illustrated a well-known technique regarding transmitting data packets between network security appliances: source authentication using a digital signature. (Franz, ¶233.) A POSITA would have been motivated to incorporate this common technique into Keohane because it is a well-known technique for authenticating data packets transmitted between network devices and was often used predictably and reliably.

Additionally, element-specific motivations to combine are discussed below.

**2. Claim 10**

A POSITA guided by Kumar would find it obvious that Keohane disclosed a flag comprising or being associated with a signature of a transmitting security element, and the receiving security element authenticating the transmitting security element based on the signature.

Kumar illustrated the common knowledge that a transmitting device could use information, such as client ID, session key, public key, etc., to create a digital signature. (See Kumar, ¶36.) The transmitting device could then use the digital

signature to create a security tag and insert it into the data packet. (*See* Kumar, ¶¶45, 46.) When the receiving device received the data packet, it could authenticate the security tag using various methods, including recreating the digital signature and comparing the result against the digital signature contained in the security tag. (*See* Kumar, ¶¶49-50; Franz, ¶236.)

A POSITA would have been motivated to incorporate this common technique of source authentication in Keohane's method. Keohane disclosed that after the receiving security element found a signature header in the data packet, it identified a trusted transmitting security element from the signature. (Keohane, ¶54.) Therefore, a POSITA would find it obvious that the receiving security element was able to authenticate the signature as being uniquely associated with the trusted transmitting security element. Although Keohane was not explicit about how the receiving security element was able to authenticate the signature and the transmitting security element, a POSITA would find it obvious that Keohane's system utilized a method of digital signature source authentication, which could be the one illustrated in Kumar. (Franz, ¶237.)

**H. Ground 8: Keohane and Chandra-2 render claims 13-14, 19-20, 25-26, and 30-31 obvious.**

The claims challenged under this ground merely require that the network security devices perform specific, well-known operations. Chandra-2 demonstrated those operations were common knowledge.

A POSITA would find it obvious that Keohane's security elements could perform Chandra-2's operations because each was well-known, commonly implemented, and would expand Keohane's range of operations. Because incorporating Chandra-2 into Keohane would merely have involved implementing common elements to yield predictable results, a POSITA would have done so.

**1. Claims 13, 19, 25, 30**

Reciting similar limitations, these claims are analyzed together.

Chandra-2 explained that a “*network security device* c[ould] be a device providing...*logging*.” (Chandra-2, ¶23.) A POSITA would have known that network traffic logging is a well-known and widely used network security operation that is especially important for forensic analysis after a vulnerability or breach has been discovered. A POSITA would have found it obvious that “logging” provided by a network security device might include “network traffic logging.” A POSITA would also have found it obvious that the security element in Keohane, as a network security device, could perform network security logging. (Franz, ¶241.)

**2. Claims 14, 20, 26, 31**

Reciting similar limitations, these claims are analyzed together.

Chandra-2 described that a “network security device c[ould] be a device providing one or more of the following features: *antivirus, intrusion prevention (IPS), content filtering, data leak prevention, antispam, antispyware...reputation-*

*based protections, event correlation, network access control, vulnerability management, load balancing and traffic shaping.*” (Chandra-2, ¶23.) In addition, Chandra-2 described that “functionality that may be provided by a network appliance include...*content filtering.*” (*Id.*, ¶24.) Indeed, the ’825 patent recognizes that DLP and IPS were well-known. (’825 patent, 9:23-26.) A POSITA would have found it obvious that Keohane’s security elements could perform any/all of these well-known operations. (Franz, ¶243.)

## IX. CONCLUSION

Accordingly, the Board should institute IPR and cancel the challenged claims.

Dated: January 31, 2023

Respectfully submitted,

/Thomas Millikan/

Lead Counsel

Thomas Millikan, Reg. No. 72,316

PERKINS COIE LLP  
11452 El Camino Real, Ste 300  
San Diego, California 92130-2080  
858.720.5700 (phone)  
858.720.5799 (fax)

Back-up Counsel  
Babak Tehrani, Reg. No. 55,937  
Andrew Klein, *PHV to be requested*  
Bingjie (Kay) Li, *PHV to be requested*

Attorneys for Netskope, Inc.

## LISTING OF CHALLENGED CLAIMS

**[1

```
] A method comprising:
```**

**[1[a]]** 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;

**[1[b]]** 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;

**[1[c]]** 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;

**[1[d][i]]** 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,

**[1[d][ii]] 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<sup>6</sup>**

[1[e]] executing, by the first network security appliance, the one or more local operations on the network traffic.

[2[a]] The method of claim 1, wherein said determining, by the first network security appliance, one or more network security operations of the first network security appliance 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

[2[b]] further comprises determining, by the first network security appliance, one or more network security operations that are to be executed by the first network security appliance except the one or more network security operations that are executed by the second network security appliance based on local network policies.

[3[a]] The method of claim 1, wherein said determining, by the first network security appliance, one or more network security operations of the

---

<sup>6</sup> The emphases denote the differences in limitation among the independent claims.

first network security appliance 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

**[3[b]]** further comprises determining, by the first network security appliance, that the one or more network security operations that are executed by the second network security appliance are to be executed by the first network security appliance.

**[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.

**[5]** The method of claim 1, wherein the flag indicates the network security operations executed by the second network security appliance.

**[6[a]]** 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

**[6[b]]** 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.

[10] The method of claim 1, wherein the flag further comprises or is associated with a signature of the second network security appliance and wherein the method further comprises authenticating, by the first network security appliance, the second network security appliance based on the signature.

[11] The method of claim 1, wherein the flag is carried in an Internet Protocol (IP) header field of the one or more packets.

[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.

[13] The method of claim 1, wherein the one or more network security operations include network traffic logging.

[14] The method of claim 1, wherein the one or more network security operations include one or more of antivirus scanning, intrusion prevention (IPS), content filtering, data leak prevention, antispam, antispyware, reputation-based protections, event correlation, network access control,

vulnerability management, load balancing, application control and traffic shaping.

**[15

```
pre]]
```** A method comprising:

**[15[a]]** 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;

**[15[b]]** 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;

**[15[c]]** 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;

**[15[d][i]]** 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,

**[15[d][ii]]** including determining one or more network security operations that are to be executed by the first network security appliance

**except the one or more network security operations that are executed by the second network security appliance based on local network polices;**  
**and**

[15[e]] executing, by the first network security appliance, the one or more local operations on the network traffic.

[16] The method of claim 15, wherein the flag indicates the network security operations executed by the second network security appliance.

[17[a]] The method of claim 15, 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

[17[b]] transmitting, by the first network security network appliance, the network traffic with the updated flag to a next network appliance participating in the CSF.

[18] The method of claim 15, 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.

[19] The method of claim 15, wherein the one or more network security operations include network traffic logging.

**[20]** The method of claim 15, wherein the one or more network security operations include one or more of antivirus scanning, intrusion prevention (IPS), content filtering, data leak prevention, antispam, antispyware, reputation-based protections, event correlation, network access control, vulnerability management, load balancing, application control and traffic shaping.

**[21[pre]]** A method comprising:

**[21[a]]** 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;

**[21[b]]** 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;

**[21[c]]** 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;

**[21[d][i]]** 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,

**[21(d)(ii)] including determining, by the first network security appliance, that the one or more network security operations that are executed by the second network security appliance are to be executed by the first network security appliance; and**

**[21(e)]** executing, by the first network security appliance, the one or more local operations on the network traffic.

**[22]** The method of claim 21, wherein the flag indicates the network security operations executed by the second network security appliance.

**[23(a)]** The method of claim 21, 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

**[23(b)]** transmitting, by the first network security network appliance, the network traffic with the updated flag to a next network appliance participating in the CSF.

**[24]** The method of claim 21, 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.

[25] The method of claim 21, wherein the one or more network security operations include network traffic logging.

[26] The method of claim 21, wherein the one or more network security operations include one or more of antivirus scanning, intrusion prevention (IPS), content filtering, data leak prevention, antispam, antispyware, reputation-based protections, event correlation, network access control, vulnerability management, load balancing, application control and traffic shaping.

[27

```
pre]] A method comprising:
```

[27[a]] 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;

[27[b][i]] 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,

[27[b][ii]] **wherein the flag indicates the network security operations executed by the second network security appliance;**

[27[c]] 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;

[27[d]] 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; and

[27[e]] executing, by the first network security appliance, the one or more local operations on the network traffic.

[28[a]] The method of claim 27, 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

[28[b]] transmitting, by the first network security network appliance, the network traffic with the updated flag to a next network appliance participating in the CSF.

[29] The method of claim 27, 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.

[30] The method of claim 27, wherein the one or more network security operations include network traffic logging.

**[31]** The method of claim 27, wherein the one or more network security operations include one or more of antivirus scanning, intrusion prevention (IPS), content filtering, data leak prevention, antispam, antispyware, reputation-based protections, event correlation, network access control, vulnerability management, load balancing, application control and traffic shaping.

**CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(d)**

Under 37 C.F.R. §42.24(d), the undersigned certifies that the word count for this *Petition for Inter Partes Review* totals 13,729 words, excluding the parts exempted by 37 C.F.R. §42.24(a).

The word count was made using the built-in word count function in the Microsoft® Word 365 software used to prepare this document.

Dated: January 31, 2023

Respectfully submitted,

/Thomas Millikan/

Lead Counsel

Thomas Millikan, Reg. No. 72,316

PERKINS COIE LLP  
11452 El Camino Real, Ste 300  
San Diego, California 92130-2080  
858.720.5700 (phone)  
858.720.5799 (fax)

Back-up Counsel  
Babak Tehrani, Reg. No. 55,937  
Andrew Klein, *PHV to be requested*  
Bingjie (Kay) Li, *PHV to be requested*

Attorneys for Netskope, Inc.

## CERTIFICATE OF SERVICE

The undersigned hereby certifies that true copies of this *PETITION FOR INTER PARTES REVIEW* and supporting materials (Exhibits 1001-1011 and Power of Attorney) have been served via Federal Express and electronically on counsel for patent owner as follows:

MICHAEL A DESANCTIS  
JAFFERY WATSON MENDONSA & HAMILTON LLP  
7501 Village Square Drive, Ste. 206  
Castle Pines, CO 80108  
mike.desanctis@jwmhlaw.com

In addition, the undersigned certifies that a true copy of the petition and supporting materials have been served on Patent Owner via email to its legal counsel:

Andrew Michael Holmes - drewholmes@quinnemanuel.com  
Jordan Brock Kaericher - jordankaericher@quinnemanuel.com  
Sean S. Pak - seanpak@quinnemanuel.com  
Tigran Guledjian - tigranguledjian@quinnemanuel.com

Dated: January 31, 2023

Respectfully submitted,

/Thomas Millikan/  
Lead Counsel  
Thomas Millikan, Reg. No. 72,316

PERKINS COIE LLP  
11452 El Camino Real, Ste 300  
San Diego, California 92130-2080  
858.720.5700 (phone)  
858.720.5799 (fax)

Back-up Counsel  
Babak Tehrani, Reg. No. 55,937  
Andrew Klein, *PHV to be requested*  
Bingjie (Kay) Li, *PHV to be requested*

Attorneys for Netskope, Inc.