



US009917856B2

(12) **United States Patent**  
**Ahn et al.**

(10) **Patent No.:** **US 9,917,856 B2**  
(45) **Date of Patent:** **Mar. 13, 2018**

(54) **RULE-BASED NETWORK-THREAT  
DETECTION FOR ENCRYPTED  
COMMUNICATIONS**

(56) **References Cited**

U.S. PATENT DOCUMENTS

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

6,098,172 A 8/2000 Coss et al.  
6,147,976 A 11/2000 Shand et al.  
6,226,372 B1 5/2001 Beebe et al.  
6,317,837 B1 11/2001 Kenworthy  
6,484,261 B1 11/2002 Wiegel  
6,611,875 B1 8/2003 Chopra et al.  
6,662,235 B1 12/2003 Callis et al.  
7,089,581 B1 8/2006 Nagai et al.

(Continued)

(72) Inventors: **David K. Ahn**, Winston-Salem, NC  
(US); **Sean Moore**, Hollis, NH (US);  
**Douglas M. DiSabello**, Leesburg, VA  
(US)

FOREIGN PATENT DOCUMENTS

(73) Assignee: **Centripetal Networks, Inc.**,  
Portsmouth, NH (US)

AU 2005328336 B2 9/2011  
AU 2006230171 B2 6/2012

(Continued)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 0 days.

OTHER PUBLICATIONS

(21) Appl. No.: **14/757,638**

Apr. 15, 2016—(US) Notice of Allowance—U.S. Appl. No.  
14/855,374.

(22) Filed: **Dec. 23, 2015**

(Continued)

(65) **Prior Publication Data**

US 2017/0187733 A1 Jun. 29, 2017

*Primary Examiner* — Jason Lee

(74) *Attorney, Agent, or Firm* — Banner & Witcoff, Ltd.

(51) **Int. Cl.**

**H04L 29/06** (2006.01)

**H04L 29/12** (2006.01)

(57) **ABSTRACT**

A packet-filtering system configured to filter packets in  
accordance with packet-filtering rules may receive data  
indicating network-threat indicators and may configure the  
packet-filtering rules to cause the packet-filtering system to  
identify packets comprising unencrypted data, and packets  
comprising encrypted data. A portion of the unencrypted  
data may correspond to one or more of the network-threat  
indicators, and the packet-filtering rules may be configured  
to cause the packet-filtering system to determine, based on  
the portion of the unencrypted data, that the packets com-  
prising encrypted data correspond to the one or more net-  
work-threat indicators.

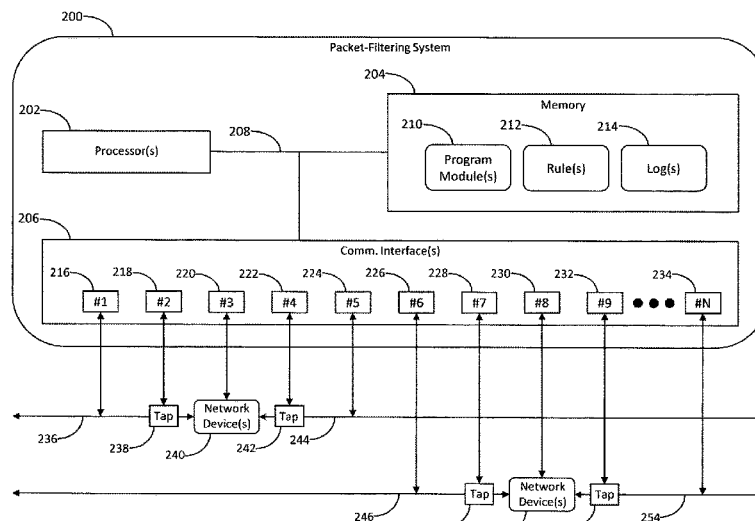
(52) **U.S. Cl.**

CPC ..... **H04L 63/1425** (2013.01); **H04L 61/1511**  
(2013.01); **H04L 63/0263** (2013.01); **H04L**  
**63/0281** (2013.01); **H04L 63/1416** (2013.01);  
**H04L 63/20** (2013.01); **H04L 69/22** (2013.01)

(58) **Field of Classification Search**

USPC ..... 713/153  
See application file for complete search history.

**25 Claims, 13 Drawing Sheets**



(56)

## References Cited

## U.S. PATENT DOCUMENTS

|                  |         |                                     |                  |         |                                      |
|------------------|---------|-------------------------------------|------------------|---------|--------------------------------------|
| 7,107,613 B1     | 9/2006  | Chen et al.                         | 2005/0251570 A1  | 11/2005 | Heasman et al.                       |
| 7,215,637 B1     | 5/2007  | Ferguson et al.                     | 2005/0286522 A1  | 12/2005 | Paddon et al.                        |
| 7,227,842 B1     | 6/2007  | Ji et al.                           | 2006/0048142 A1  | 3/2006  | Roesse et al.                        |
| 7,237,267 B2     | 6/2007  | Rayes et al.                        | 2006/0053491 A1  | 3/2006  | Khuti et al.                         |
| 7,263,099 B1     | 8/2007  | Woo et al.                          | 2006/0070122 A1  | 3/2006  | Bellovin                             |
| 7,299,353 B2     | 11/2007 | Le Pennec et al.                    | 2006/0104202 A1  | 5/2006  | Reiner                               |
| 7,331,061 B1     | 2/2008  | Ramsey et al.                       | 2006/0114899 A1  | 6/2006  | Toumura et al.                       |
| 7,478,429 B2     | 1/2009  | Lyon                                | 2006/0136987 A1  | 6/2006  | Okuda                                |
| 7,539,186 B2     | 5/2009  | Aerrabotu et al.                    | 2006/0137009 A1  | 6/2006  | Chesla                               |
| 7,610,621 B2     | 10/2009 | Turley et al.                       | 2006/0146879 A1  | 7/2006  | Anthias et al.                       |
| 7,684,400 B2     | 3/2010  | Govindarajan et al.                 | 2006/0195896 A1  | 8/2006  | Fulp et al.                          |
| 7,710,885 B2     | 5/2010  | Ilnicki et al.                      | 2006/0212572 A1  | 9/2006  | Afek et al.                          |
| 7,721,084 B2     | 5/2010  | Salminen et al.                     | 2006/0248580 A1  | 11/2006 | Fulp et al.                          |
| 7,818,794 B2     | 10/2010 | Wittman                             | 2006/0262798 A1  | 11/2006 | Joshi et al.                         |
| 7,954,143 B2     | 5/2011  | Aaron                               | 2007/0083924 A1  | 4/2007  | Lu                                   |
| 8,004,994 B1     | 8/2011  | Darisi et al.                       | 2007/0211644 A1  | 9/2007  | Ottamalika et al.                    |
| 8,037,517 B2     | 10/2011 | Fulp et al.                         | 2007/0240208 A1  | 10/2007 | Yu et al.                            |
| 8,042,167 B2     | 10/2011 | Fulp et al.                         | 2008/0005795 A1  | 1/2008  | Acharya et al.                       |
| 8,117,655 B2     | 2/2012  | Spielman                            | 2008/0043739 A1  | 2/2008  | Suh et al.                           |
| 8,176,561 B1     | 5/2012  | Hurst et al.                        | 2008/0072307 A1  | 3/2008  | Maes                                 |
| 8,306,994 B2     | 11/2012 | Kenworthy                           | 2008/0077705 A1  | 3/2008  | Li et al.                            |
| 8,495,725 B2     | 7/2013  | Ahn                                 | 2008/0163333 A1  | 7/2008  | Kasralikar                           |
| 8,726,379 B1     | 5/2014  | Stiansen et al.                     | 2008/0229415 A1  | 9/2008  | Kapoor et al.                        |
| 8,806,638 B1     | 8/2014  | Mani                                | 2008/0235755 A1  | 9/2008  | Blaisdell et al.                     |
| 8,856,926 B2     | 10/2014 | Narayanaswamy et al.                | 2008/0279196 A1  | 11/2008 | Friskney et al.                      |
| 8,935,785 B2     | 1/2015  | Pandurangi                          | 2008/0301765 A1  | 12/2008 | Nicol et al.                         |
| 9,094,445 B2     | 7/2015  | Moore et al.                        | 2009/0138938 A1  | 5/2009  | Harrison et al.                      |
| 9,124,552 B2     | 9/2015  | Moore                               | 2009/0172800 A1  | 7/2009  | Wool                                 |
| 9,137,205 B2     | 9/2015  | Rogers et al.                       | 2009/0222877 A1  | 9/2009  | Diehl et al.                         |
| 9,154,446 B2     | 10/2015 | Gemelli et al.                      | 2009/0240698 A1  | 9/2009  | Shukla et al.                        |
| 9,160,713 B2     | 10/2015 | Moore                               | 2009/0328219 A1  | 12/2009 | Narayanaswamy                        |
| 2001/0039579 A1  | 11/2001 | Trcka et al.                        | 2010/0011433 A1  | 1/2010  | Harrison et al.                      |
| 2001/0039624 A1  | 11/2001 | Kellum                              | 2010/0011434 A1  | 1/2010  | Kay                                  |
| 2002/0016858 A1  | 2/2002  | Sawada et al.                       | 2010/0082811 A1  | 4/2010  | Van Der Merwe et al.                 |
| 2002/0038339 A1  | 3/2002  | Xu                                  | 2010/0095367 A1  | 4/2010  | Narayanaswamy                        |
| 2002/0049899 A1  | 4/2002  | Kenworthy                           | 2010/0107240 A1  | 4/2010  | Thaler et al.                        |
| 2002/0164962 A1  | 11/2002 | Mankins et al.                      | 2010/0132027 A1  | 5/2010  | Ou                                   |
| 2002/0165949 A1  | 11/2002 | Na et al.                           | 2010/0199346 A1  | 8/2010  | Ling et al.                          |
| 2002/0186683 A1  | 12/2002 | Buck et al.                         | 2010/0211678 A1  | 8/2010  | McDysan et al.                       |
| 2002/0198981 A1  | 12/2002 | Corl et al.                         | 2010/0232445 A1  | 9/2010  | Bellovin                             |
| 2003/0035370 A1  | 2/2003  | Brustoloni                          | 2010/0242098 A1  | 9/2010  | Kenworthy                            |
| 2003/0097590 A1  | 5/2003  | Syvanne                             | 2010/0268799 A1  | 10/2010 | Maestas                              |
| 2003/0105976 A1  | 6/2003  | Copeland                            | 2010/0296441 A1  | 11/2010 | Barkan                               |
| 2003/0120622 A1  | 6/2003  | Nurmela et al.                      | 2010/0303240 A1  | 12/2010 | Beachem et al.                       |
| 2003/0123456 A1  | 7/2003  | Denz et al.                         | 2011/0055916 A1  | 3/2011  | Ahn                                  |
| 2003/0142681 A1  | 7/2003  | Chen et al.                         | 2011/0055923 A1  | 3/2011  | Thomas                               |
| 2003/0145225 A1  | 7/2003  | Bruton et al.                       | 2011/0088092 A1  | 4/2011  | Nguyen et al.                        |
| 2003/0154297 A1  | 8/2003  | Suzuki et al.                       | 2011/0141900 A1  | 6/2011  | Jayawardena et al.                   |
| 2003/0154399 A1  | 8/2003  | Zuk et al.                          | 2011/0185055 A1  | 7/2011  | Nappier et al.                       |
| 2003/0188192 A1  | 10/2003 | Tang et al.                         | 2011/0270956 A1  | 11/2011 | McDysan et al.                       |
| 2003/0212900 A1  | 11/2003 | Liu et al.                          | 2012/0023576 A1* | 1/2012  | Sorensen ..... G06F 21/577<br>726/22 |
| 2004/0010712 A1  | 1/2004  | Hui et al.                          | 2012/0106354 A1  | 5/2012  | Pleshek et al.                       |
| 2004/0073655 A1  | 4/2004  | Kan et al.                          | 2012/0113987 A1  | 5/2012  | Riddoch et al.                       |
| 2004/0088542 A1  | 5/2004  | Daude et al.                        | 2012/0240135 A1  | 9/2012  | Risbood et al.                       |
| 2004/0093513 A1  | 5/2004  | Cantrell et al.                     | 2012/0264443 A1  | 10/2012 | Ng et al.                            |
| 2004/0098511 A1  | 5/2004  | Lin et al.                          | 2012/0314617 A1  | 12/2012 | Erichsen et al.                      |
| 2004/0151155 A1  | 8/2004  | Jouppi                              | 2012/0331543 A1  | 12/2012 | Bostrom et al.                       |
| 2004/0177139 A1  | 9/2004  | Schuba et al.                       | 2013/0047020 A1  | 2/2013  | Hershko et al.                       |
| 2004/0193943 A1  | 9/2004  | Angelino et al.                     | 2013/0059527 A1  | 3/2013  | Hasesaka et al.                      |
| 2004/0199629 A1* | 10/2004 | Bomer ..... G06F 11/362<br>709/224  | 2013/0061294 A1  | 3/2013  | Kenworthy                            |
| 2004/0205360 A1  | 10/2004 | Norton et al.                       | 2013/0117852 A1  | 5/2013  | Stute                                |
| 2004/0250124 A1  | 12/2004 | Chesla et al.                       | 2013/0254766 A1  | 9/2013  | Zuo et al.                           |
| 2005/0010765 A1  | 1/2005  | Swander et al.                      | 2013/0305311 A1  | 11/2013 | Puttaswamy Naga et al.               |
| 2005/0024189 A1  | 2/2005  | Weber                               | 2014/0075510 A1  | 3/2014  | Sonoda et al.                        |
| 2005/0108557 A1  | 5/2005  | Kayo et al.                         | 2014/0115654 A1  | 4/2014  | Rogers et al.                        |
| 2005/0114704 A1  | 5/2005  | Swander                             | 2014/0201123 A1  | 7/2014  | Ahn et al.                           |
| 2005/0117576 A1  | 6/2005  | McDysan et al.                      | 2014/0215574 A1  | 7/2014  | Erb et al.                           |
| 2005/0125697 A1  | 6/2005  | Tahara                              | 2014/0281030 A1  | 9/2014  | Cui et al.                           |
| 2005/0138204 A1  | 6/2005  | Iyer et al.                         | 2014/0283004 A1  | 9/2014  | Moore                                |
| 2005/0138353 A1* | 6/2005  | Spies ..... H04L 63/0442<br>713/153 | 2014/0283030 A1  | 9/2014  | Moore et al.                         |
| 2005/0141537 A1  | 6/2005  | Kumar et al.                        | 2014/0317397 A1  | 10/2014 | Martini                              |
| 2005/0183140 A1  | 8/2005  | Goddard                             | 2014/0366132 A1  | 12/2014 | Stiansen et al.                      |
| 2005/0229246 A1  | 10/2005 | Rajagopal et al.                    | 2015/0207813 A1* | 7/2015  | Reybok ..... G06F 21/552<br>726/22   |
|                  |         |                                     | 2015/0237012 A1  | 8/2015  | Moore                                |
|                  |         |                                     | 2015/0304354 A1  | 10/2015 | Rogers et al.                        |

(56)

**References Cited****U.S. PATENT DOCUMENTS**

2015/0334125 A1 11/2015 Bartos et al.  
 2015/0350229 A1 12/2015 Mitchell  
 2015/0373043 A1 12/2015 Wang et al.

**FOREIGN PATENT DOCUMENTS**

|    |             |    |         |
|----|-------------|----|---------|
| CA | 2600236     | A1 | 10/2006 |
| EP | 1006701     | A2 | 6/2000  |
| EP | 1313290     | A1 | 5/2003  |
| EP | 1484884     | A2 | 12/2004 |
| EP | 1677484     | A2 | 7/2006  |
| EP | 2385676     | A1 | 11/2011 |
| EP | 2498442     | A1 | 9/2012  |
| EP | 1864226     | B1 | 5/2013  |
| KR | 20010079361 | A  | 8/2001  |
| WO | 2005046145  | A1 | 5/2005  |
| WO | 2006093557  | A2 | 9/2006  |
| WO | 2006105093  | A2 | 10/2006 |
| WO | 2007109541  | A2 | 9/2007  |
| WO | 2011038420  | A2 | 3/2011  |
| WO | 2012146265  | A1 | 11/2012 |

**OTHER PUBLICATIONS**

ISR for PCT/US2013/057502, dated Nov. 7, 2013.  
 International Search Report off International Application No. PCT/US2014/023286, dated Jun. 24, 2014.  
 ISR off International Application No. PCT/US2013/072566, dated Mar. 24, 2014.  
 ISR off International Application No. PCT/US2014/027723, dated Jun. 26, 2014.  
 "Control Plane Policing Implementation Best Practices"; Cisco Systems; Mar. 13, 2013; <[https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp\\_gs.html](https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html)>.  
 Reumann, John; "Adaptive Packet Filters"; IEEE, 2001, Department of Electrical Engineering and Computer Science, the University of Michigan, Ann Arbor, MI.  
 Greenwald, Michael; "Designing an Academic Firewall: Policy, Practice, and Experience with SURF"; IEEE, Proceedings of SNDSS, 1996.  
 Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, Jan. 2005. Second IEEE Consumer Communications and Networking Conference, pp. 599-601.  
 "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Division 2012 Principal Investigators' Meeting"; Sean Moore, Oct. 10, 2014.  
 John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Inc.; Nov. 5, 2010, pp. 1-26.  
 Palo Alto Networks; "Designing a Zero Trust Network With Next-Generation Firewalls"; pp. 1-10; last viewed on Oct. 21, 2012.  
 Jan. 11, 2016—(US) Non Final Rejection—U.S. Appl. No. 14/698,560.  
 Apr. 27, 2011—(WO) International Search Report and Written Opinion—App PCT/US2010/054520.  
 Mar. 4, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/316,331.  
 Mar. 3, 2011—(EP) Communication Pursuant to Rules 70(2) and 70a(2)—App 06758213.0.  
 Feb. 14, 2011—(EP) Search Report—App 06758213.0.  
 Fulp, Errin; "Errin Fulp," XP002618346, [www.cs.wfu.edu/fulp/ewfPub.html](http://www.cs.wfu.edu/fulp/ewfPub.html), pp. 1-5 (Copyright 2010).  
 Sep. 30, 2010—(US) Office Action—U.S. Appl. No. 11/390,976.  
 Sep. 10, 2010—(AU) Office Action—App 2006230171.  
 Aug. 20, 2010—(AU) Office Action—App 2005328336.  
 Jun. 23, 2010—(US) Final Rejection—U.S. Appl. No. 11/316,331.  
 Apr. 29, 2010—(US) Interview Summary—U.S. Appl. No. 11/390,976.  
 Mar. 26, 2010—(US) Final Rejection—U.S. Appl. No. 11/390,976.  
 Sep. 14, 2009 (US) Office Action—U.S. Appl. No. 11/316,331.  
 Jun. 24, 2009—(US) Office Action—U.S. Appl. No. 11/390,976.  
 Jul. 3, 2008—(WO) Written Opinion of the International Searching Authority—App PCT/US06/11291.  
 Aug. 31, 2007—(EP) Communication Pursuant to Rules 109 and 110—App 05857614.1.  
 Acharya et al., "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pp. 1-11 (2007).  
 Sep. 11, 2006—(WO) Written Opinion of the International Searching Authority—App PCT/US05/47008.  
 Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Wake Forest University, pp. 1-6 (2006).  
 Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005).  
 E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Science Department, Wake Forest University, Jan. 2004.  
 E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004.  
 E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004.  
 E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded Sep. 2003.  
 E. Al-Shaer et al., "Firewall Policy Advisor for Anomaly Discovery and Rule Editing", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, 2003.  
 V.P. Ranganath, "A Set-Based Approach to Packet Classification", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, 889-894, 2003.  
 M. Christiansen et al., "Using IDSs for Packet Filtering", Technical Report, BRICS, Oct. 2002.  
 Lee et al., "Development Framework for Firewall Processors," IEEE, pp. 352-355 (2002).  
 L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM SIGMETRICS, Jun. 2001.  
 D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001.  
 E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001.  
 S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001.  
 G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001.  
 P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001.  
 D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): Feb. 2000.  
 A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000.  
 X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000.  
 A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000.  
 O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000.  
 J. Xu et al., "Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications", IEEE Journal on Selected Areas in Communications, 17(6): 1190-1200, Jun. 1999.

(56)

**References Cited****OTHER PUBLICATIONS**

- C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999.
- R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999.
- S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999.
- J. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998.
- V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998.
- M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997.
- S.M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994.
- W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1): 15, 1994.
- G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991.
- M. Al-Suwaiyel et al., "Algorithms for Tile Compaction", ACM Transactions on Database Systems, 9(2): 243-263, Jun. 1984.
- D. Corner, "Analysis of a Heuristic for Full Tile Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sep. 1981.
- R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979.
- E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion oTime Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978.
- J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35, 1978.
- R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976.
- W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956.
- Bellion, "High Performance Packet Classification", <http://www.hipac.org> (Publication Date Unknown).
- Oct. 18, 2011—(EP) Communication Pursuant to Article 94(3)—App 06 758 213.0.
- Jun. 9, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/390,976.
- Jun. 26, 2012—(EP) Extended Search Report—App 05857614.1.
- Jun. 9, 2012—(AU) Notice of Acceptance—App 2006230171.
- Nov. 11, 2011—(AU) Second Office Action—App 2006230171.
- Jan. 17, 2013—(CA) Office Action—App 2,600,236.
- Jan. 16, 2013—(CA) Office Action—App 2,594,020.
- Nov. 20, 2012—(EP) Communication under rule 71(3)—App 06 758 213.0.
- Apr. 18, 2013—(EP) Decision to Grant a European Patent—App 06758212.0.
- Aug. 25, 2011—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
- Feb. 6, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
- Aug. 7, 2012—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
- Nov. 26, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
- Apr. 4, 2013—(US) Notice of Allowance—U.S. Appl. No. 12/871,806.
- Jan. 14, 2015—(EP) Extended Search Report—App 10819667.6.
- May 26, 2014—(CA) Office Action—App 2010297968.
- May 25, 2015—(AU) Notice of Acceptance—App 2010297968.
- May 14, 2015—(US) Non Final Rejection—U.S. Appl. No. 13/940,240.
- Nov. 27, 2015—(US) Final Rejection—U.S. Appl. No. 13/940,240.
- Jul. 10, 2015—(WO) Communication Relating to the Results of the Partial International Search for International App—PCT/US2015/024691.
- Jul. 23, 2015—(WO) International Preliminary Report on Patentability—App PCT/US2013/072566.
- Jan. 28, 2016—(WO) International Search Report and Written Opinion—App PCT/US2015/062691.
- International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated Sep. 16, 2015.
- International Preliminary Report on Patentability for International App. No. PCT/US2013/057502, dated Apr. 28, 2015.
- International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated Sep. 15, 2015.
- International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated Sep. 15, 2015.
- Dec. 22, 2015—(US) Final Office Action—U.S. Appl. No. 14/714,207.
- Feb. 26, 2016—(US) Non Final Office Action—U.S. Appl. No. 14/253,992.
- Nov. 2, 2015—(AU) Office Action—App 2013372879.
- Apr. 26, 2016—(US) Office Action—U.S. Appl. No. 14/745,207.
- May 6, 2016—(US) Office Action—U.S. Appl. No. 14/714,207.
- May 13, 2016—(US) Office Action—U.S. Appl. No. 13/940,240.
- Jun. 14, 2016—(US) Office Action—U.S. Appl. No. 14/625,486.
- Feb. 25, 2016—(AU) Office Action—App 2014249055.
- Feb. 24, 2016—(AU) Office Action—App 2014228257.
- Jun. 9, 2016—(WO) International Search Report—PCT/US2016/026339.
- Jun. 16, 2016—(CA) Office Action—App 2,888,935.
- Jul. 11, 2016—(EP) Office Action—App 14720824.3.
- Jul. 22, 2016—(US) Office Action—U.S. Appl. No. 14/921,718.
- Jul. 20, 2016—(AU) Office Action—App 2013335255.
- Oct. 5, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/698,560.
- Sep. 13, 2016—(CA) Office Action—App 2,902,206.
- Sep. 14, 2016—(CA) Office Action—App 2,897,737.
- Sep. 26, 2016—(CA) Office Action—App 2,902,158.
- Oct. 26, 2016—(US) Office Action—U.S. Appl. No. 13/940,240.
- Nov. 21, 2016—(US) Office Action—U.S. Appl. No. 14/745,207.
- Dec. 5, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/714,207.
- Singh, Rajeev et al. "Detecting and Reducing the Denial of Service attacks in WLANs", Dec. 2011, World Congress on Information and Communication TEchnologies, pp. 968-973.
- Feb. 10, 2017—(US) Notice of Allowance—U.S. Appl. No. 14/625,486.
- Feb. 15, 2017—(US) Notice of Allowance—U.S. Appl. No. 14/921,718.
- Mar. 6, 2017—(WO) International Search Report and Written Opinion—App PCT/US2016/068008.
- Jun. 7, 2017—(US) Office Action—U.S. Appl. No. 14/745,207.
- Sep. 4, 2015 (US) Notice of Allowance—U.S. Appl. No. 14/702,755.
- Jun. 7, 2017—(WO) International Search Report and Written Opinion—App PCT/US2016/067111.

\* cited by examiner

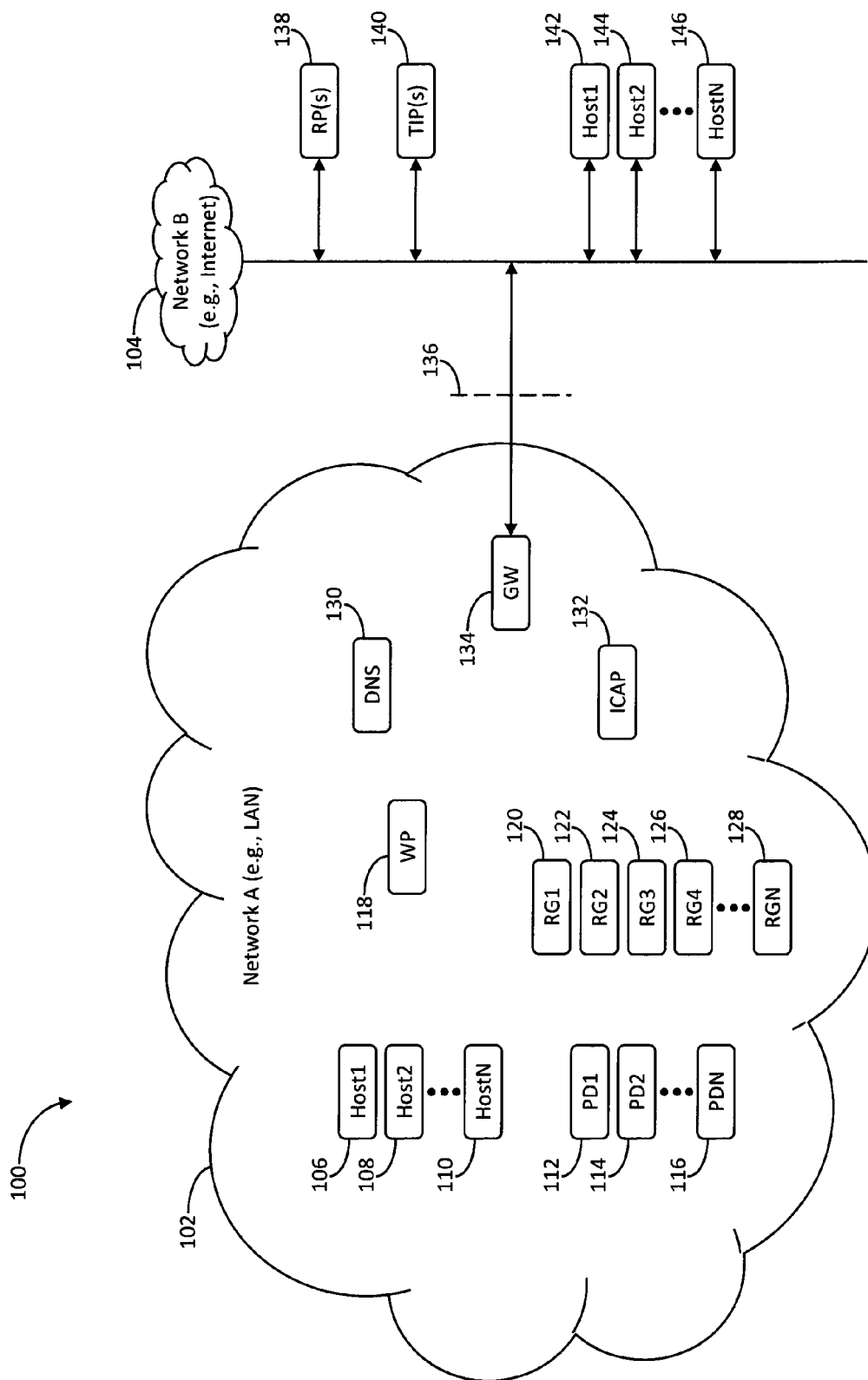


FIG. 1

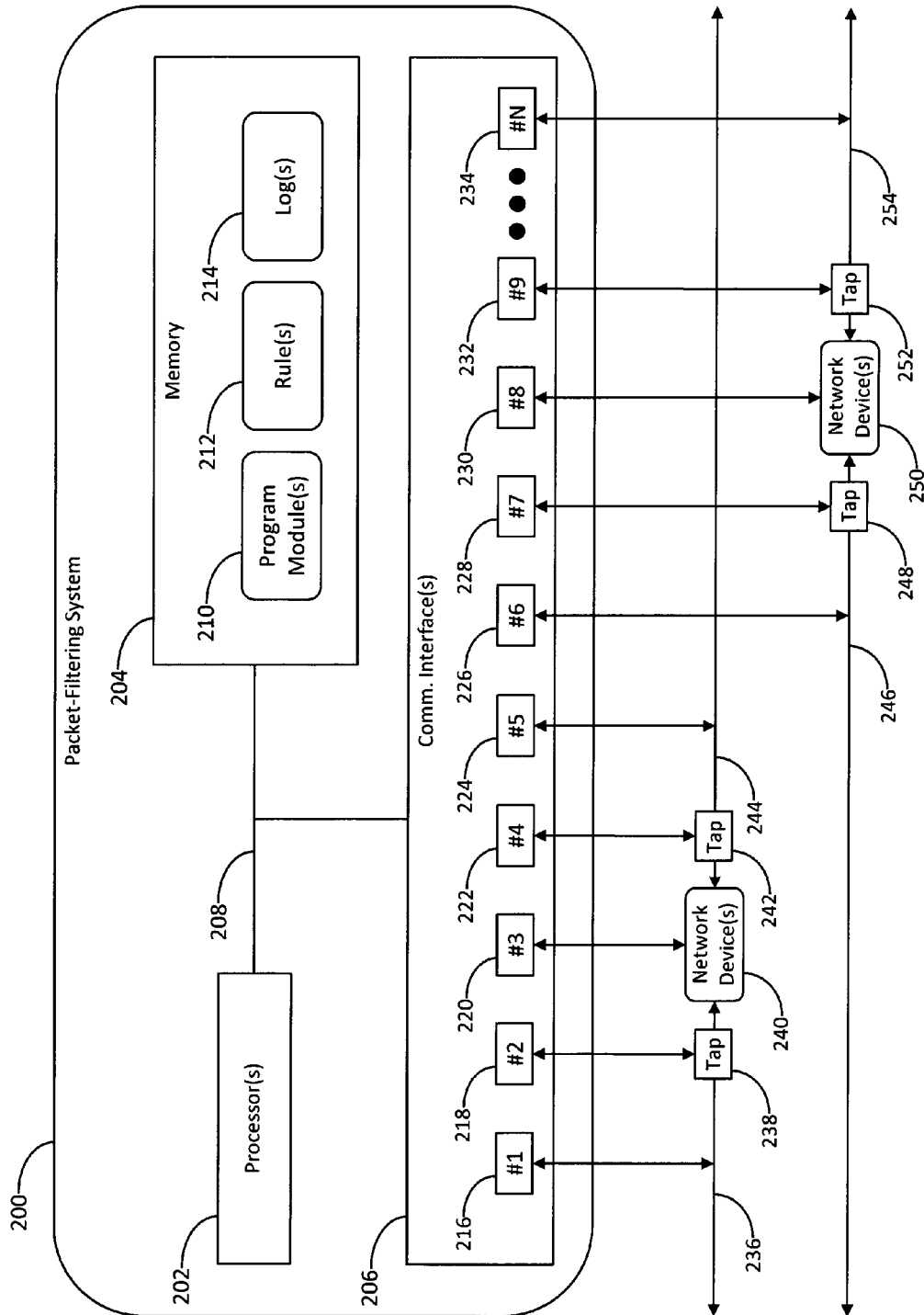


FIG. 2

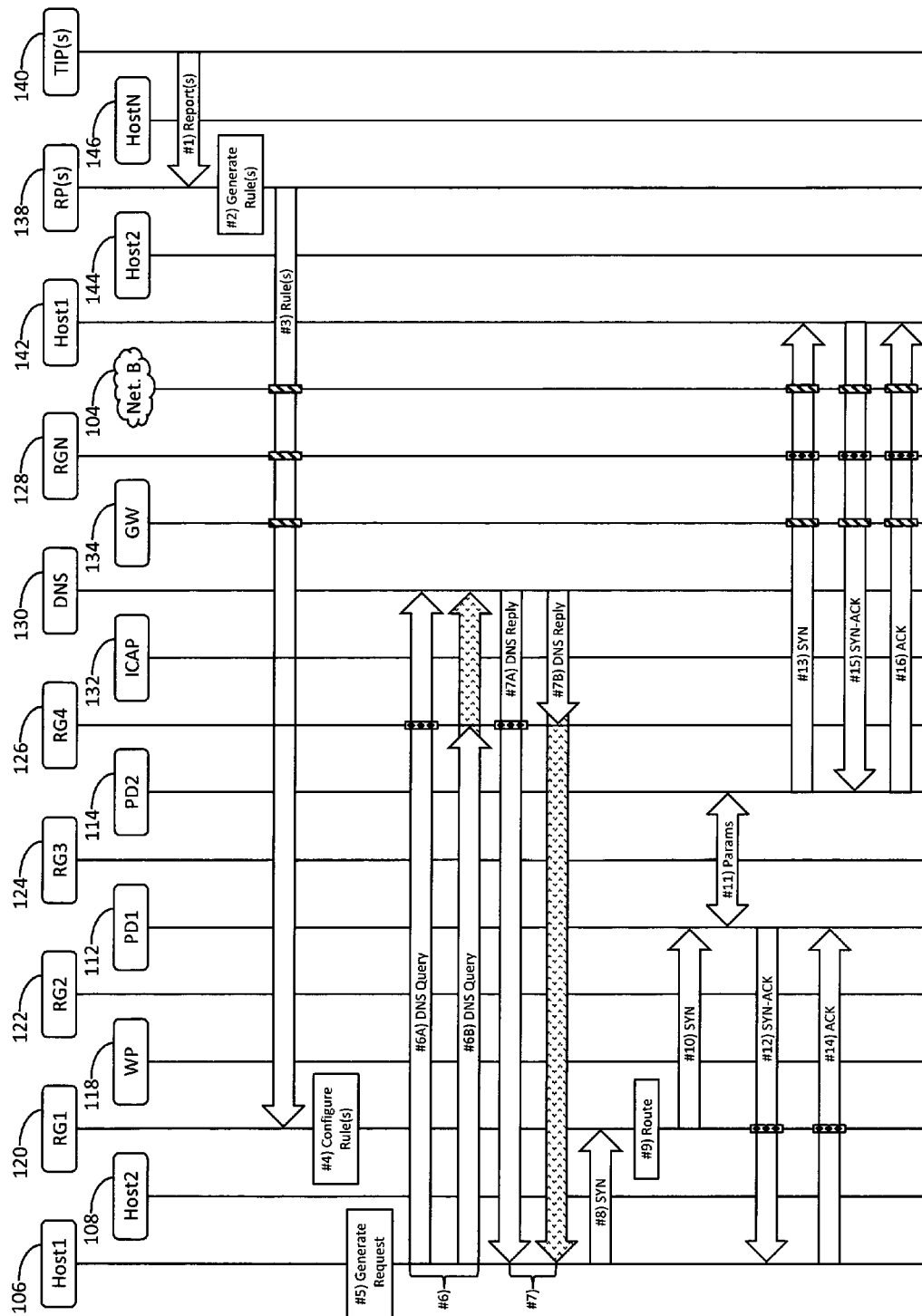


FIG. 3A

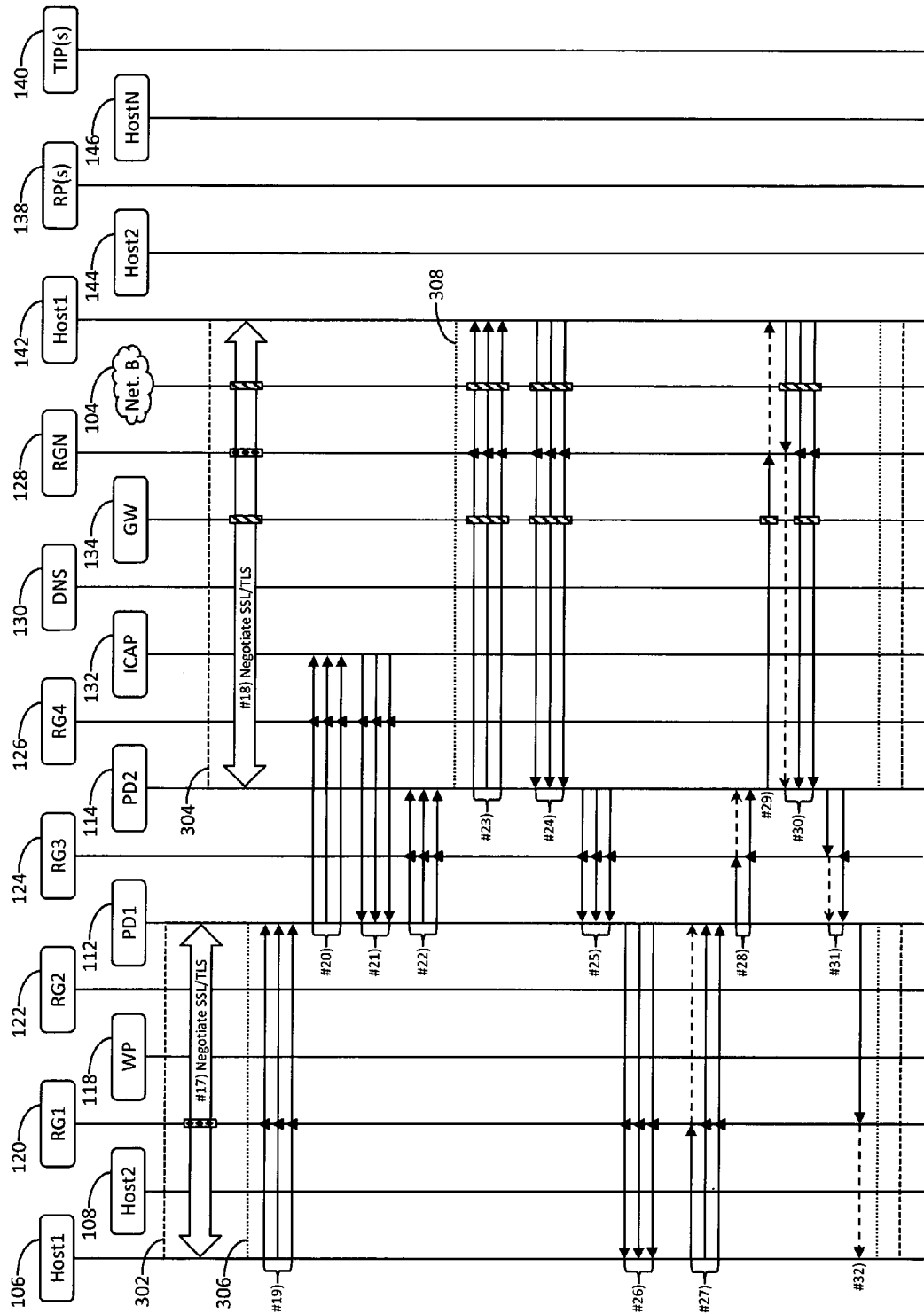


FIG. 3B

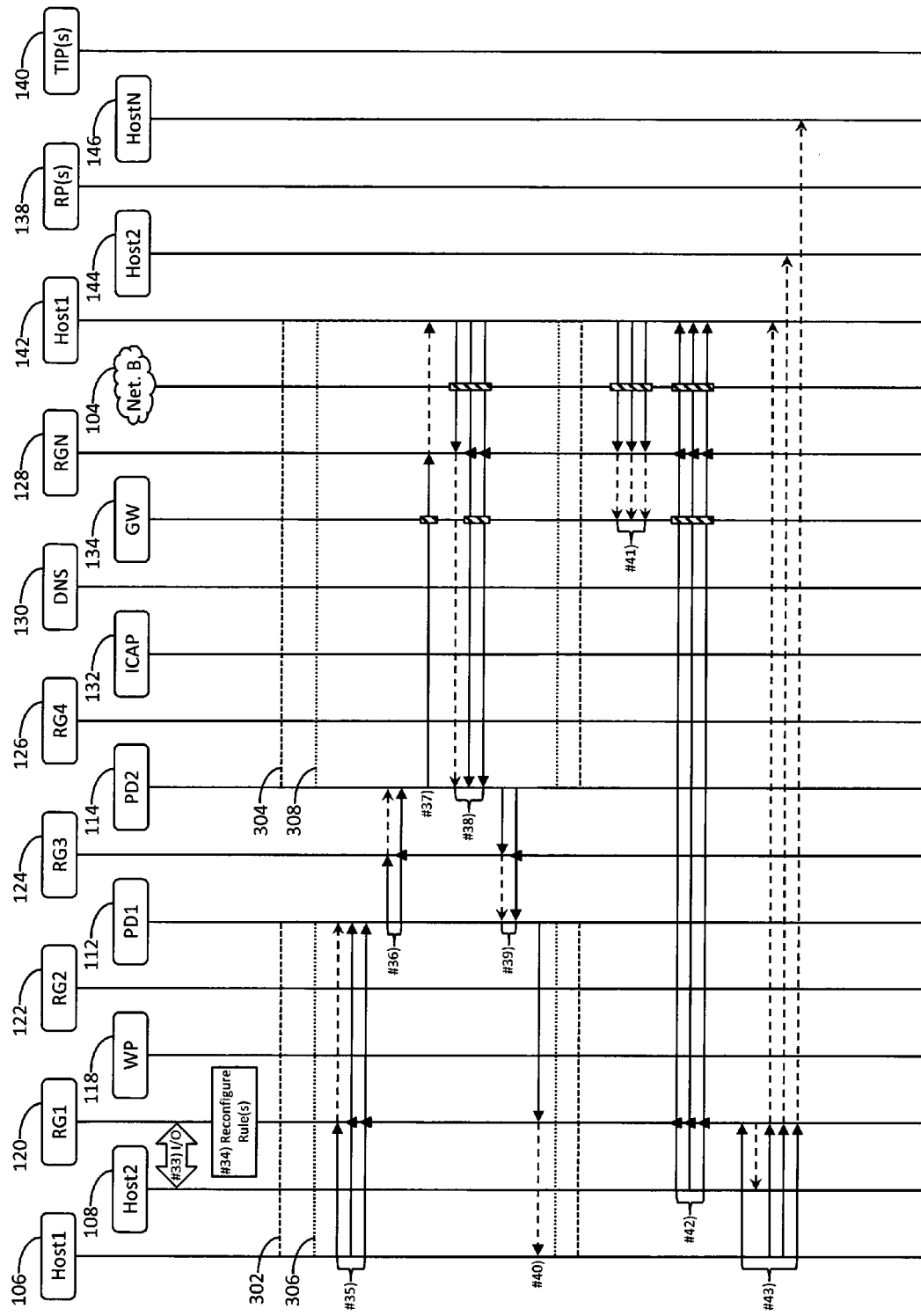


FIG. 3C

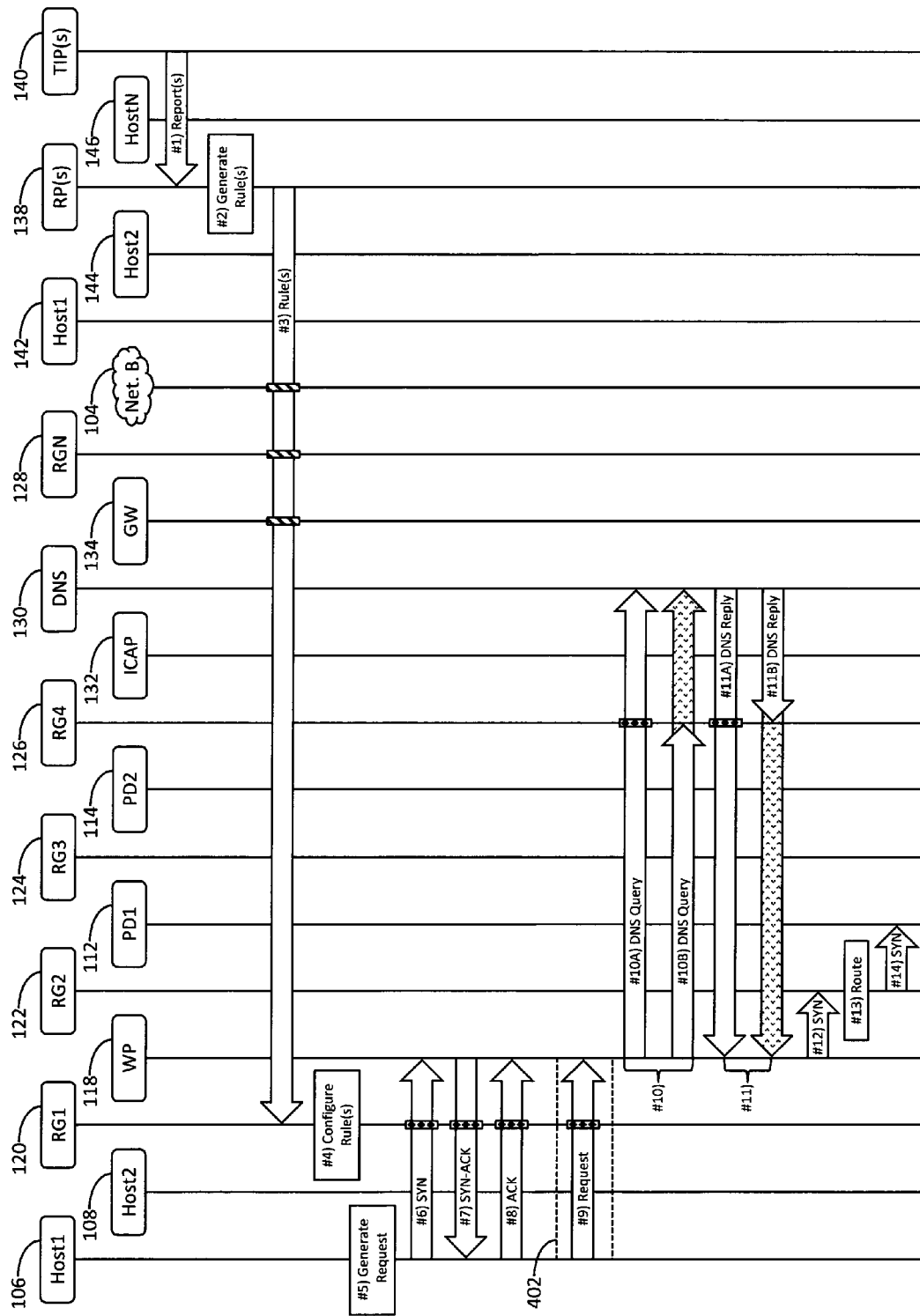


FIG. 4A

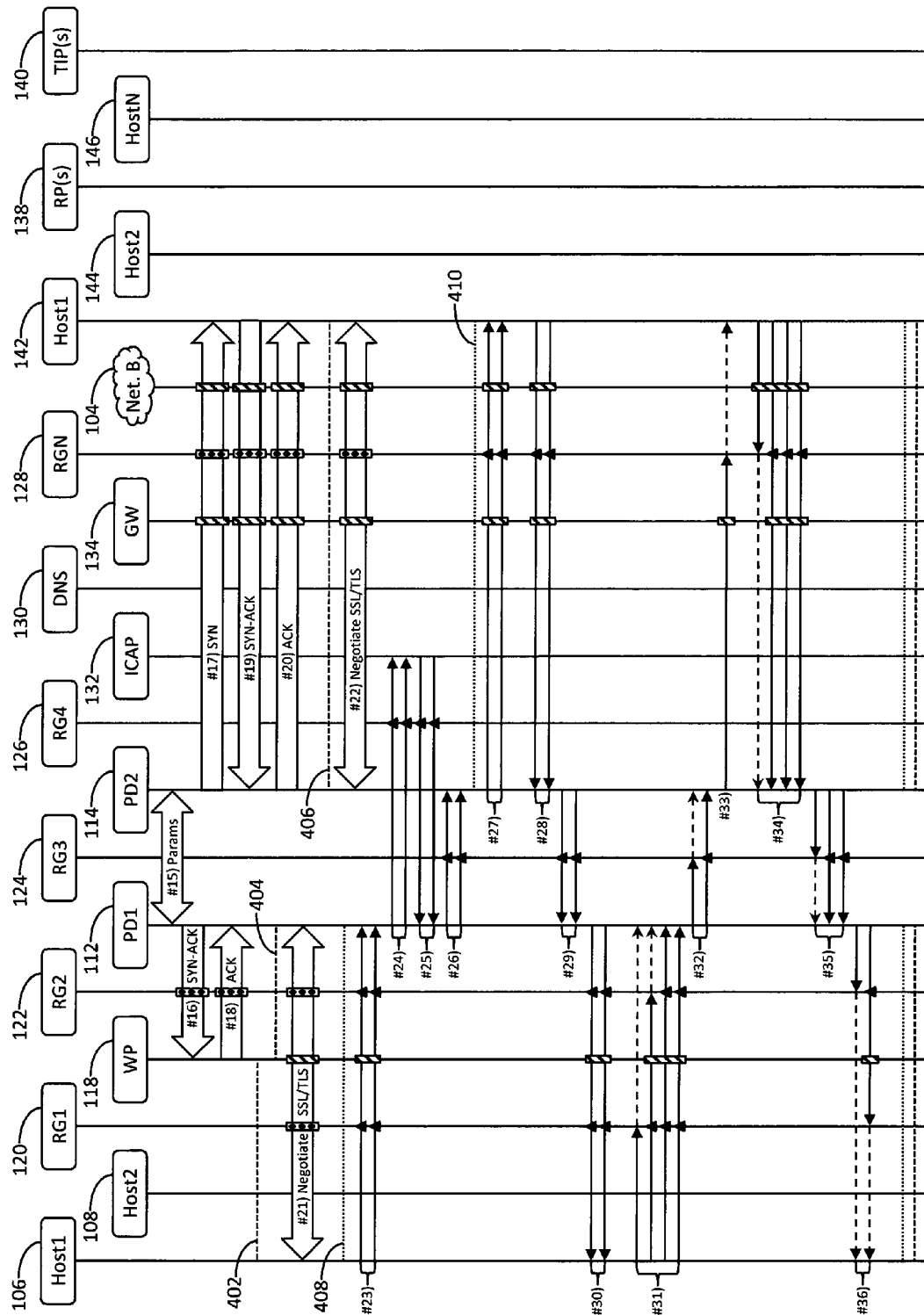


FIG. 4B

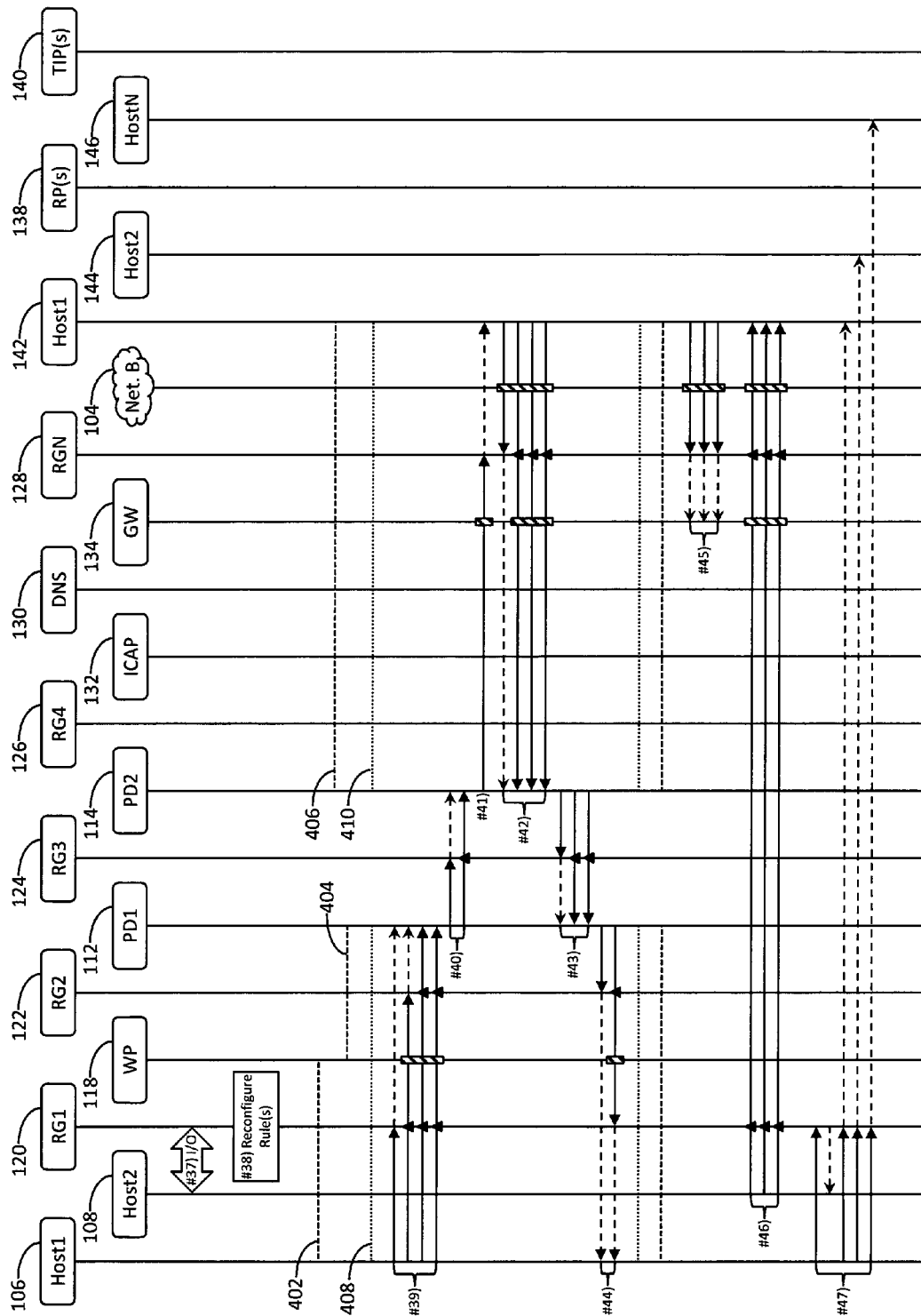


FIG. 4C

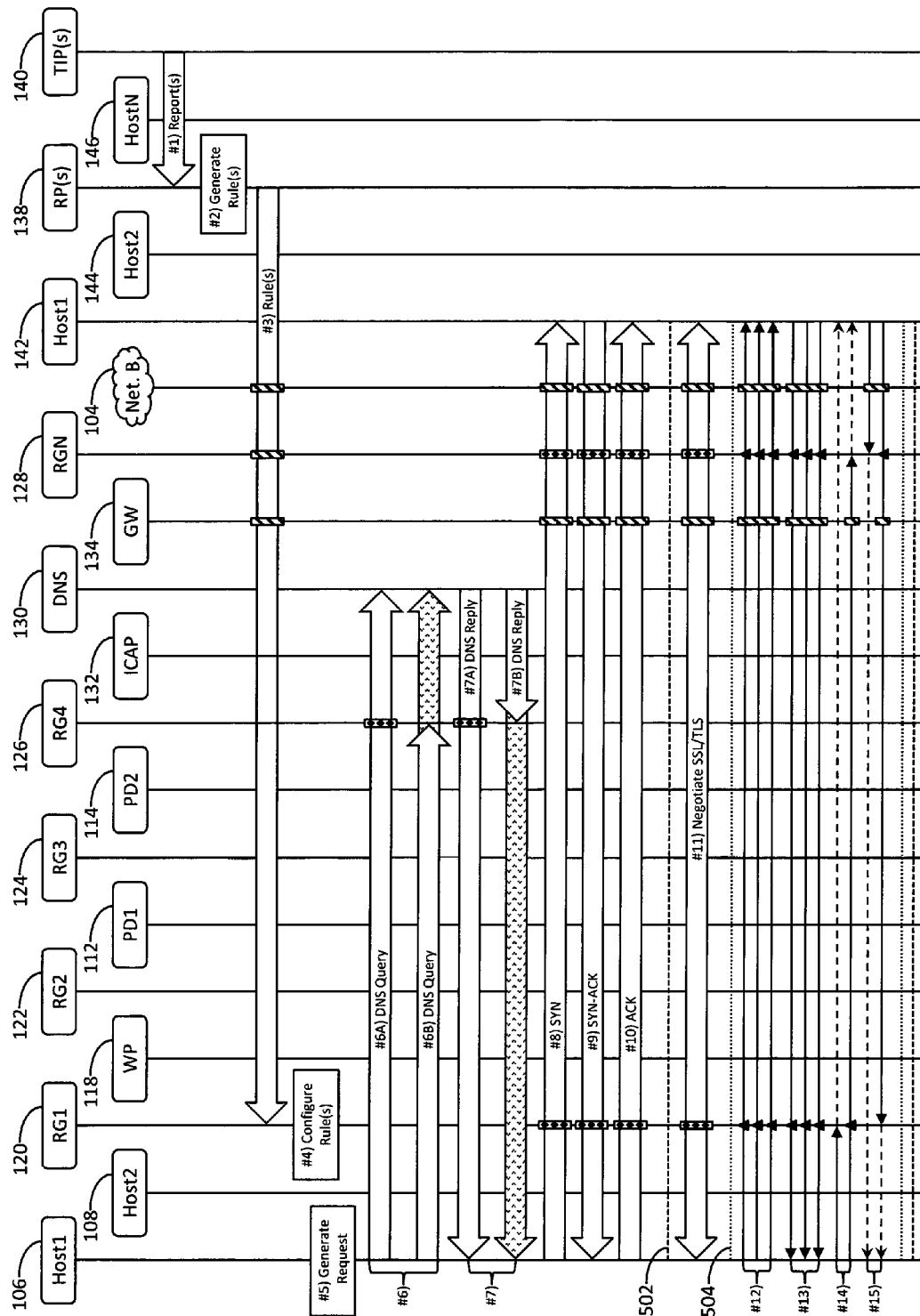


FIG. 5A

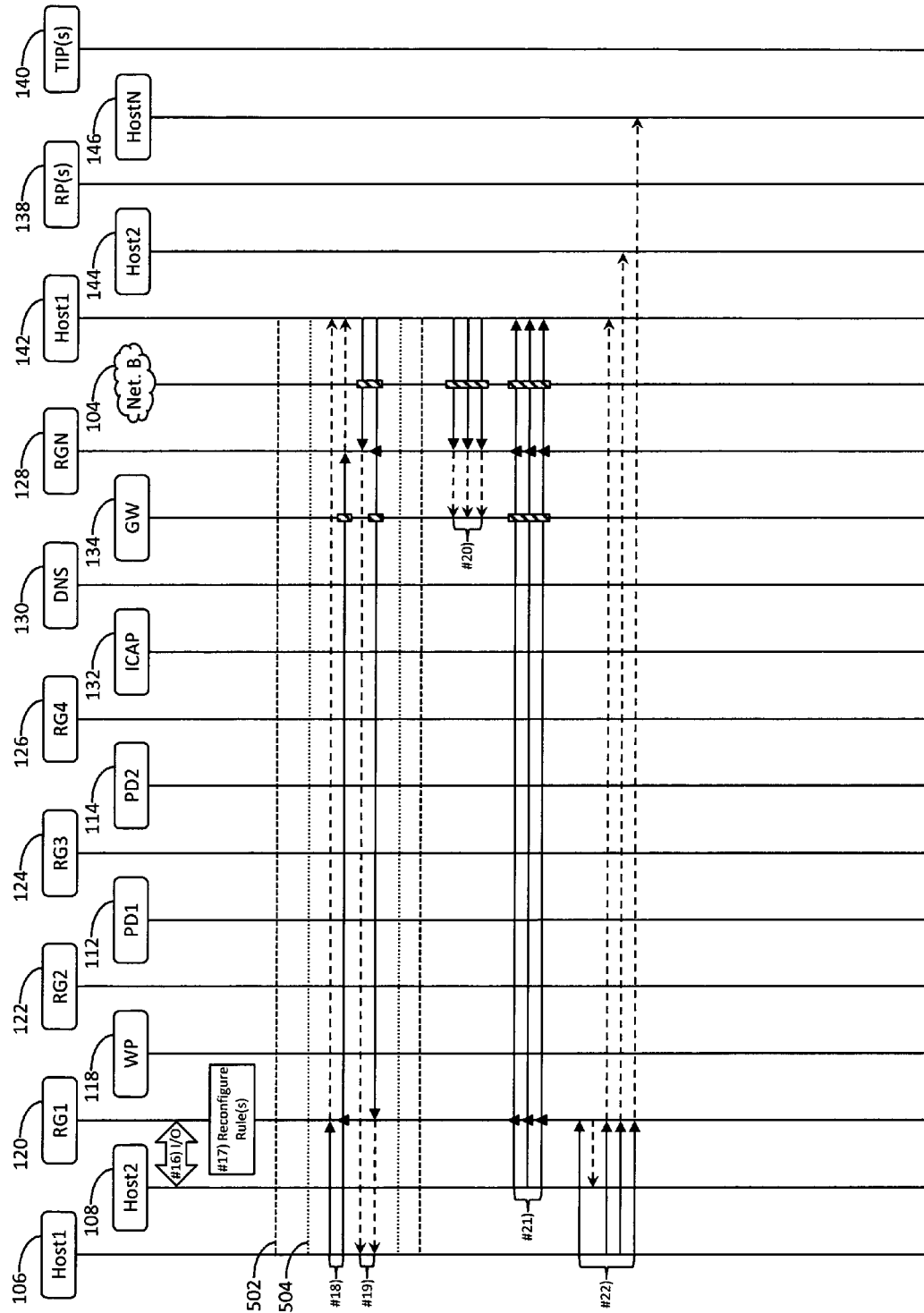


FIG. 5B

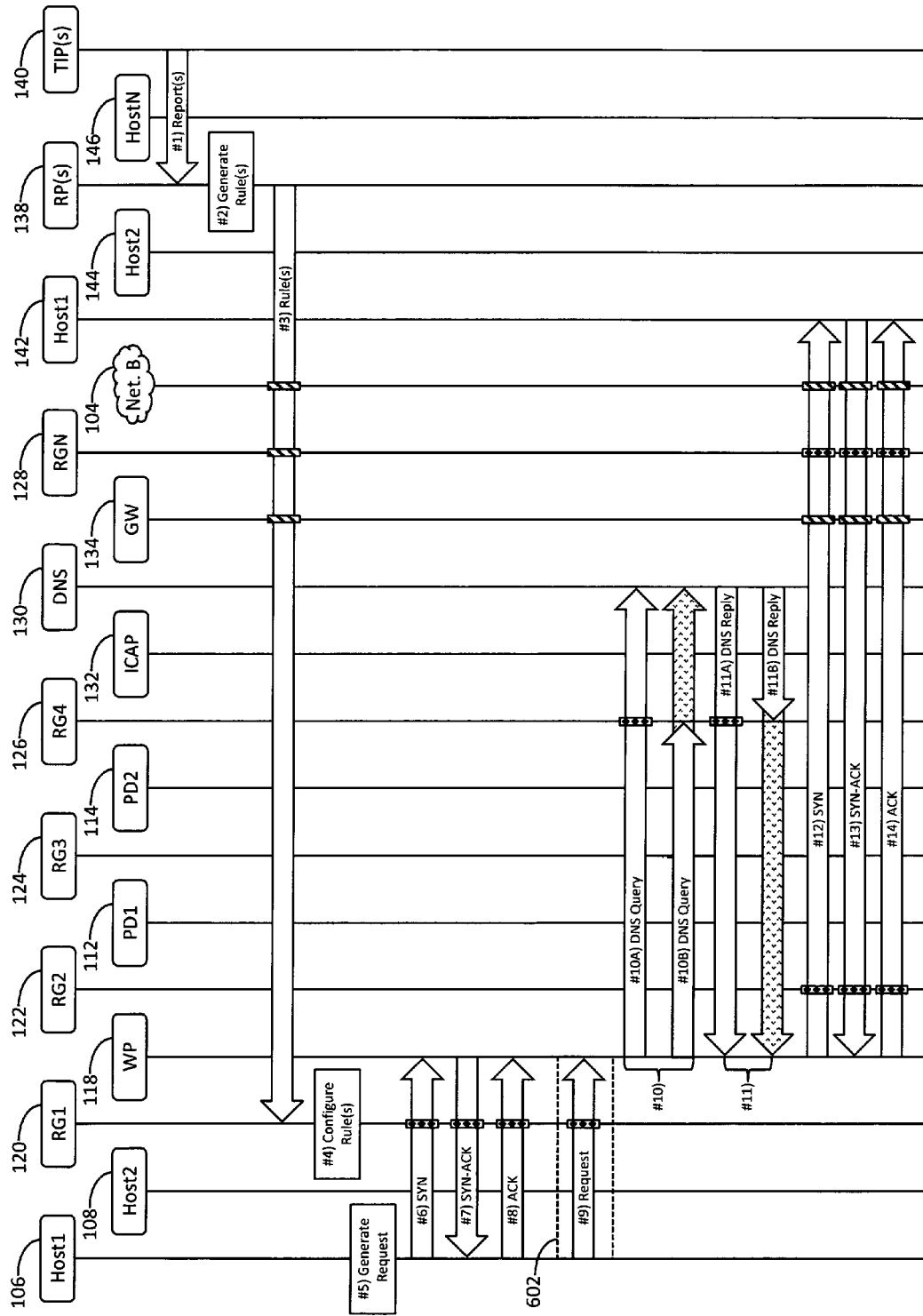


FIG. 6A

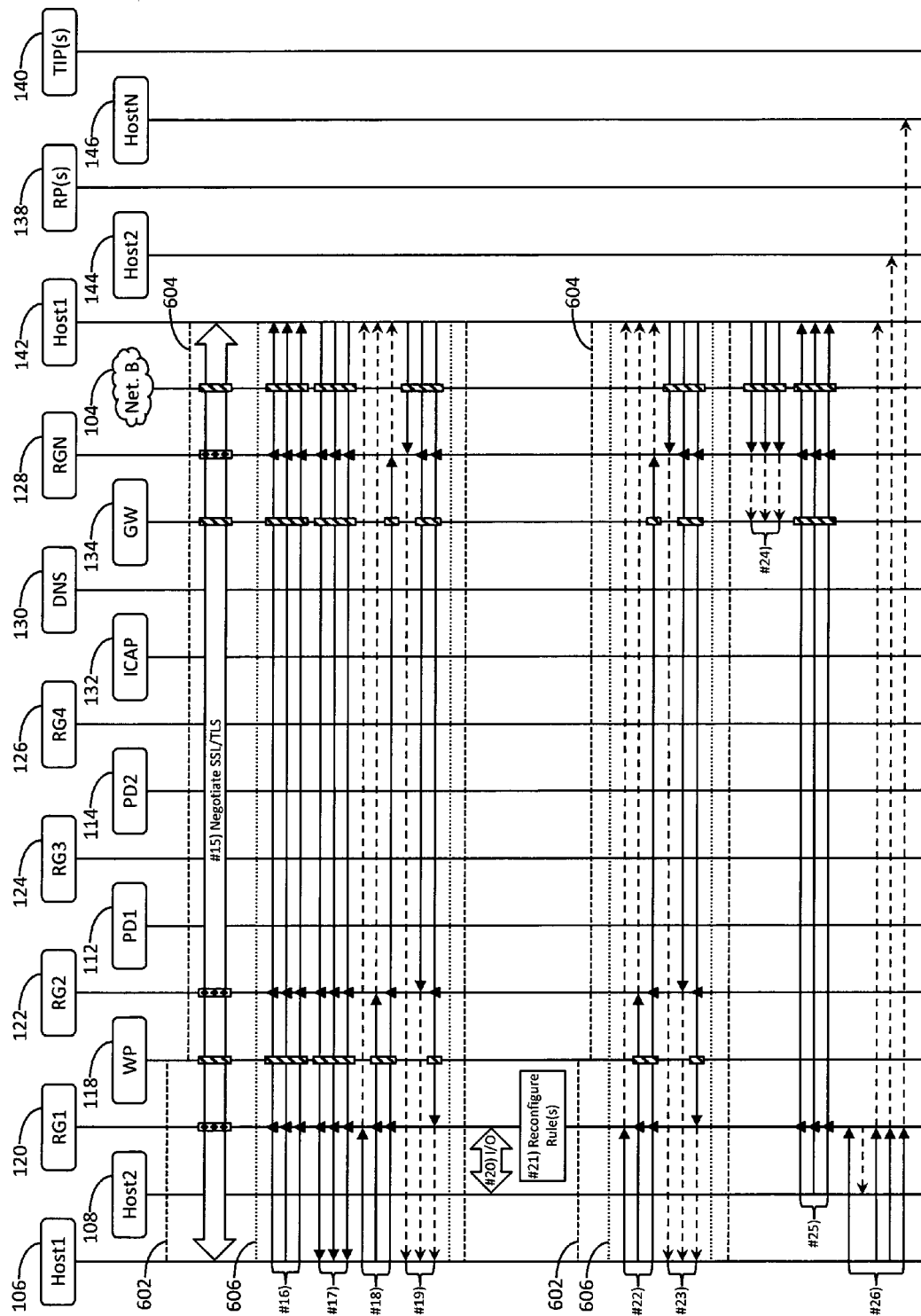


FIG. 6B

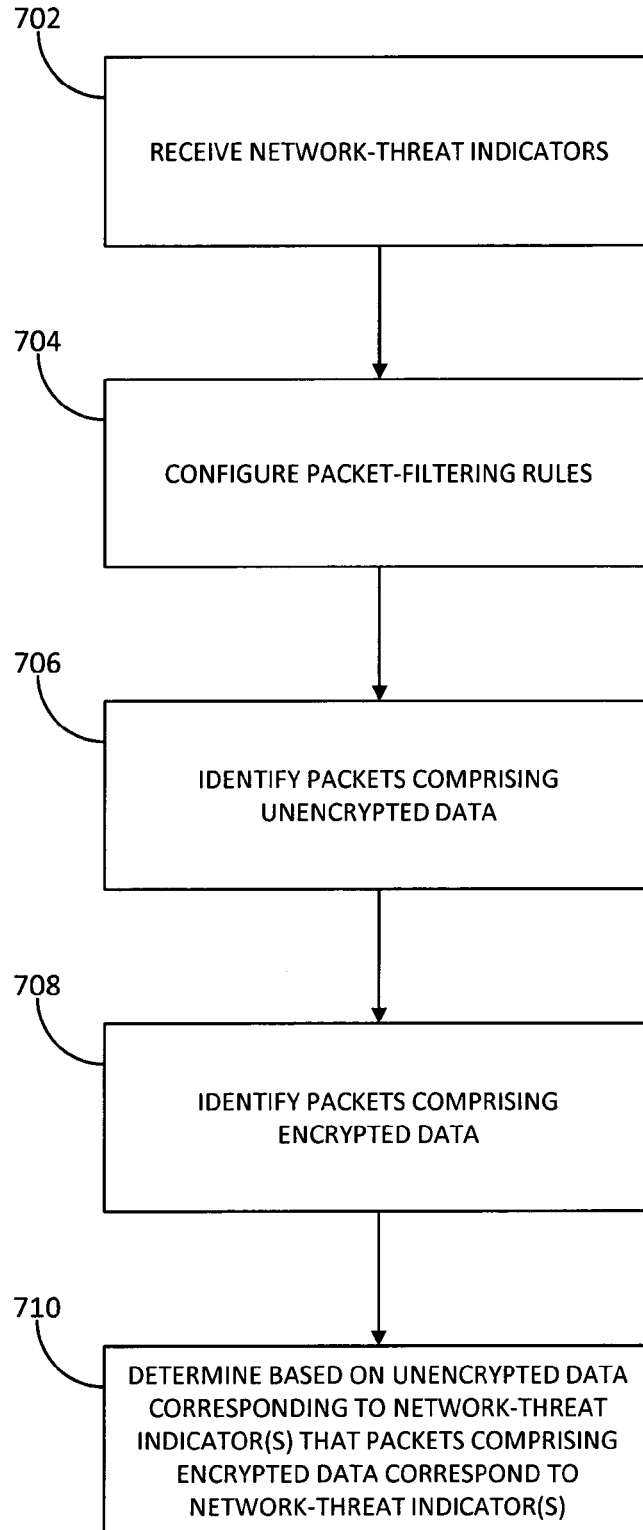


FIG. 7

1

# RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS

## BACKGROUND

Network security is becoming increasingly important as the information age continues to unfold. Network threats may take a variety of forms (e.g., unauthorized requests or data transfers, viruses, malware, large volumes of traffic designed to overwhelm resources, and the like). Network-threat services provide information associated with network threats, for example, reports that include listings of network-threat indicators (e.g., network addresses, domain names, uniform resource identifiers (URIs), and the like). Such information may be utilized to identify network threats. Encrypted communications, however, may obfuscate data corresponding to network threats. Accordingly, there is a need for rule-based network-threat detection for encrypted communications.

## SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is intended neither to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts of the disclosure in a simplified form as a prelude to the description below.

Aspects of this disclosure relate to rule-based network-threat detection for encrypted communications. In accordance with embodiments of the disclosure, a packet-filtering system configured to filter packets in accordance with packet-filtering rules may receive data indicating network-threat indicators and may configure the packet-filtering rules to cause the packet-filtering system to identify packets comprising unencrypted data, and packets comprising encrypted data. A portion of the unencrypted data may correspond to one or more of the network-threat indicators, and the packet-filtering rules may be configured to cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

## BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements, and wherein:

FIG. 1 depicts an illustrative environment for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure;

FIG. 2 depicts an illustrative packet-filtering system for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure;

FIGS. 3A-C, 4A-C, 5A-B, and 6A-B depict illustrative event sequences for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure; and

2

FIG. 7 depicts an illustrative method for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure.

## DETAILED DESCRIPTION

In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the disclosure.

Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless. In this respect, the specification is not intended to be limiting.

FIG. 1 depicts an illustrative environment for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to FIG. 1, environment 100 may include networks 102 and 104. Network 102 may comprise one or more networks (e.g., Local Area Networks (LANs), Wide Area Networks (WANs), Virtual Private Networks (VPNs), or combinations thereof) associated with one or more individuals or entities (e.g., governments, corporations, service providers, or other organizations). Network 104 may comprise one or more networks (e.g., LANs, WANs, VPNs, or combinations thereof) that interface network 102 with one or more other networks (not illustrated). For example, network 104 may comprise the Internet, a similar network, or portions thereof.

Environment 100 may also include one or more hosts, such as computing or network devices (e.g., servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, firewalls, switches, access points, or the like). For example, network 102 may include hosts 106, 108, and 110, proxy devices 112, 114, and 116, web proxy 118, rule gates 120, 122, 124, 126, and 128, domain name system (DNS) 130, Internet content adaptation protocol (ICAP) server 132, and gateway 134. As used herein, “host” (or “hosts”) refers to any type of network device (or node) or computing device; while such devices may be assigned (or configured to be assigned) one or more network-layer addresses, the term “host” (or “hosts”) does not imply such devices necessarily are assigned (or configured to be assigned) one or more network-layer addresses.

Gateway 134 may be located at border 136 between networks 102 and 104 and may interface network 102 or one or more hosts located therein with network 104 or one or more hosts located therein. For example, network 104 may include one or more rule providers 138, one or more threat-intelligence providers 140, and hosts 142, 144, and 146, and gateway 134 may interface hosts 106, 108, and 110, proxy devices 112, 114, and 116, web proxy 118, rule gates 120, 122, 124, 126, and 128, DNS 130, and ICAP server 132 with rule providers 138, threat-intelligence providers 140, and hosts 142, 144, and 146.

FIG. 2 depicts an illustrative packet-filtering system for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to FIG. 2, packet-filtering system 200 may be associated with network 102 and may include one or more of rule gates 120, 122, 124, 126, and 128. Packet-filtering system 200 may comprise one or more processors

202, memory 204, one or more communication interfaces 206, and data bus 208. Data bus 208 may interface processors 202, memory 204, and communication interfaces 206. Memory 204 may comprise one or more program modules 210, rules 212, and logs 214. Program modules 210 may comprise instructions that when executed by processors 202 cause packet-filtering system 200 to perform one or more of the functions described herein. Rules 212 may comprise one or more packet-filtering rules in accordance with which packet-filtering system 200 is configured to filter packets received via communication interfaces 206. Logs 214 may include one or more entries generated by processors 202 in accordance with rules 212 for packets received by packet-filtering system 200 via communication interfaces 206.

Communication interfaces 206 may interface packet-filtering system 200 with one or more communication links of environment 100 (e.g., of networks 102 and 104). In some embodiments, one or more of communication interfaces 206 may interface directly with a communication link of environment 100. For example, interfaces 216 and 224 may interface directly with links 236 and 244, respectively. In some embodiments, one or more of communication interfaces 206 may interface indirectly with a communication link of environment 100. For example, interface 220 may interface with links 236 and 244 via one or more network devices 240. Network devices 240 may provide interface 220 with access to (or copies of) packets traversing one or more of links 236 and 244, for example, via a switched port analyzer (SPAN) port of network devices 240. Additionally or alternatively, interfaces 218 and 222 may interface with links 236 and 244 via tap devices 238 and 242. For example, packet-filtering system 200 may provision tap device 238 with one or more of rules 212 configured to cause tap device 238 to identify packets traversing link 236 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 218, and packet-filtering system 200 may provision tap device 242 with one or more of rules 212 configured to cause tap device 242 to identify packets traversing link 244 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 222. Similarly, interfaces 226 and 234 may interface directly with links 246 and 254, respectively; network devices 250 may provide interface 230 with access to (or copies of) packets traversing one or more of links 246 and 254; packet-filtering system 200 may provision tap device 248 with one or more of rules 212 configured to cause tap device 248 to identify packets traversing link 246 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 228; and packet-filtering system 200 may provision tap device 252 with one or more of rules 212 configured to cause tap device 252 to identify packets traversing link 254 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 232. In some embodiments, packet-filtering system 200 may comprise one or more of tap devices 238, 242, 248, and 252 or network devices 240 and 250.

FIGS. 3A-C, 4A-C, 5A-B, and 6A-B depict illustrative event sequences for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. The depicted steps are merely illustrative and may be omitted, combined, or performed in an order other than that depicted; the numbering of the steps is merely for ease of reference and does not imply any particular ordering is necessary or preferred.

Referring to FIG. 3A, at step #1, threat-intelligence providers 140 may communicate one or more threat-intelligence reports to rule providers 138. The threat-intelligence

reports may include one or more network-threat indicators, for example, domain names (e.g., fully qualified domain names (FQDNs)), URIs, network addresses, or the like. At step #2, rule providers 138 may utilize the threat-intelligence reports to generate one or more packet-filtering rules configured to identify packets comprising data corresponding to the network-threat indicators. At step #3, rule providers 138 may communicate the packet-filtering rules to rule gate 120. As indicated by the crosshatched boxes over the lines extending downward from network 104, rule gate 128, and gateway 134, the packet-filtering rules may traverse network 104, rule gate 128, and gateway 134. For example, network 104 and gateway 134 may interface rule providers 138 and rule gate 120, and rule gate 128 may interface a communication link interfacing network 104 and gateway 134. Rule gate 120 may receive the packet-filtering rules generated by rule providers 138 and, at step #4, may utilize the received packet-filtering rules to configure rules 212 to cause packet-filtering system 200 to identify packets comprising data corresponding to at least one of the plurality of network-threat indicators.

At step #5, host 106 may generate a request. For example, host 106 may execute a web browser, and the web browser may generate a request in response to user input (e.g., navigation of the web browser to a URI). The request may comprise a domain name, and host 106 may generate a DNS query comprising the domain name and, at step #6, may communicate the DNS query toward DNS 130. Rule gate 126 may interface a communication link interfacing host 106 and DNS 130, the domain name included in the request may correspond to one or more of the network-threat indicators, and rules 212 may be configured to cause rule gate 126 to one or more of identify one or more packets comprising the DNS query, determine that the packets comprise the domain name corresponding to the network-threat indicators, and responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, one or more of log (as indicated by the diamond-patterned box over the line extending downward from rule gate 126) or drop the packets. Rule gate 126 may generate log data (e.g., one or more entries in logs 214) for the packets. For example, the packets may comprise a network address of host 106 (e.g., as a source address in their network-layer headers), and rule gate 126 may generate log data indicating the network address of host 106. As depicted by step #6A, the packets may be communicated to DNS 130. In some embodiments, rules 212 may be configured to cause rule gate 126 to, responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching DNS 130, as depicted by step #6B.

DNS 130 may generate a reply to the DNS query and, at step #7, may communicate the reply toward host 106. The reply may comprise the domain name corresponding to the network-threat indicators, and rules 212 may be configured to cause rule gate 126 to one or more of identify one or more packets comprising the reply, determine that the packets comprise the domain name corresponding to the network-threat indicators, and responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, one or more of log or drop the packets. Rule gate 126 may generate log data (e.g., one or more entries in logs 214) for the packets. For example, the packets may comprise the network address of host 106 (e.g., as a destination address in

5

their network-layer headers), and rule gate 126 may generate log data indicating the network address of host 106. Similarly, the domain name may correspond to host 142, the packets may comprise a network address of host 142 (e.g., DNS 130 may have resolved the domain name included in the query to the network address of host 142), and rule gate 126 may generate log data indicating the network address of host 142. As depicted by step #7A, the packets may be communicated to host 106. In some embodiments, rules 212 may be configured to cause rule gate 126 to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching host 106, as depicted by step #7B.

Packet-filtering system 200 may be configured to correlate packets identified by packet-filtering system 200 (e.g., the packets comprising the reply to the DNS query) with packets previously identified by packet-filtering system 200 (e.g., the packets comprising the DNS query). For example, packet-filtering system 200 may be configured to determine that packets identified by packet-filtering system 200 (e.g., the packets comprising the reply to the DNS query) are one or more of associated with, related to, or the product of packets previously identified by packet-filtering system 200 (e.g., the packets comprising the DNS query). Packet-filtering system 200 may be configured to correlate packets identified by packet-filtering system 200 with packets previously identified by packet-filtering system 200 based on data stored in logs 214 (e.g., the log data generated by rule gate 126 in steps #6 and #7).

For example, for one or more packets logged by packet-filtering system 200 (e.g., the packets comprising the DNS query or the packets comprising the reply to the DNS query), logs 214 may comprise one or more entries indicating one or more of network-layer information (e.g., information derived from one or more network-layer header fields of the packets, such as a protocol type, a destination network address, a source network address, a signature or authentication information (e.g., information from an Internet protocol security (IPsec) encapsulating security payload (ESP)), or the like), transport-layer information (e.g., a destination port, a source port, a checksum or similar data (e.g., error detection or correction values, such as those utilized by the transmission control protocol (TCP) or the user datagram protocol (UDP)), or the like), application-layer information (e.g., information derived from one or more application-layer header fields of the packets, such as a domain name, a uniform resource locator (URL), a uniform resource identifier (URI), an extension, a method, state information, media-type information, a signature, a key, a timestamp, an application identifier, a session identifier, a flow identifier, sequence information, authentication information, or the like), other data in the packets (e.g., payload data), or one or more environmental variables (e.g., information associated with but not solely derived from the packets themselves, such as one or more arrival (or receipt) or departure (or transmission) times of the packets (e.g., at or from one or more of rule gates 120, 122, 124, 126, or 128, tap devices 238, 242, 248, or 252, or network devices 240 or 250), one or more ingress or egress identifiers (e.g., associated with one or more physical or logical network interfaces, ports, or communication-media types of one or more of rule gates 120, 122, 124, 126, or 128, tap devices 238, 242, 248, or 252, or network devices 240 or 250 via which the packets were one or more of received or transmitted), one or more device identifiers (e.g., associated with one or more of rule gates 120, 122, 124, 126, or 128, tap devices 238, 242, 248,

6

or 252, or network devices 240 or 250 via which the packets were one or more of received or transmitted), or the like), and packet-filtering system 200 may utilize such entries to correlate one or more packets identified by packet-filtering system 200 with one or more packets previously identified by packet-filtering system 200.

In some embodiments, packet-filtering system 200 may implement one or more aspects of the technology described in U.S. patent application Ser. No. 14/618,967, filed Feb. 10, 2015, and entitled "CORRELATING PACKETS IN COMMUNICATIONS NETWORKS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology (e.g., to correlate one or more packets identified by packet-filtering system 200 with one or more packets previously identified by packet-filtering system 200).

Host 106 may generate one or more packets destined for host 142 comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between hosts 106 and 142 and, at step #8, may communicate the packets toward host 142. Rule gate 120 may interface a communication link interfacing hosts 106 and 142, and rules 212 may be configured to cause rule gate 120 to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs 214 (e.g., the log data generated by rule gate 126 in one or more of steps #6 or #7).

At step #9, rule gate 120 may route the packets comprising the data configured to establish the connection between hosts 106 and 142 to proxy device 112 and, at step #10, may communicate the packets to proxy device 112. For example, rules 212 may be configured to cause rule gate 120 to route the packets to proxy device 112 based on data in the packets, for example, one or more ports (e.g., port 443) indicated by transport-layer headers in the packets, indicating the connection between hosts 106 and 142 will be utilized to establish an encrypted communication session or tunnel (e.g., a session established in accordance with the transport layer security (TLS) protocol, secure sockets layer (SSL) protocol, secure shell (SSH) protocol, or the like). In some embodiments, rules 212 may be configured to cause rule gate 120 to route the packets to proxy device 112 based on a determination that one or more of hosts 106 or 142 is associated with a network address for which rules 212 indicate encrypted communications should be established via one or more of proxy devices 112, 114, or 116. For example, proxy devices 112, 114, and 116 may be part of a proxy system (e.g., a SSL/TLS proxy system) that enables packet-filtering system 200 to filter packets comprising encrypted data based on information within the encrypted data, and rules 212 may be configured to cause rule gate 120 to route the packets to proxy device 112 based on a determination that host 142 is associated with a network address of a domain corresponding to the network-threat indicators.

Additionally or alternatively, network 102 may include one or more hosts for which rules 212 indicate connections utilized to establish encrypted communication sessions (e.g., connections with hosts corresponding to network-threat indicators) should be established via one or more of proxy devices 112, 114, or 116, as well as one or more hosts for which rules 212 indicate connections utilized to establish encrypted communication sessions should not be established

via one or more of proxy devices **112**, **114**, and **116**, for example, hosts that generate sensitive data (e.g., personally identifiable information (PII)), inspection of which may present privacy or regulatory concerns (e.g., data subject to the health insurance portability and accountability act (HIPAA), or the like), and rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on a determination that host **106** is associated with a network address for which rules **212** indicate encrypted communications should be established via one or more of proxy devices **112**, **114**, or **116**.

For example, link **236** may interface host **106** with rule gate **120**, link **244** may interface rule gate **120** with host **142**, link **246** may interface rule gate **120** with proxy device **112**, link **254** may interface proxy devices **112** and **114** and may comprise a communication link internal to a proxy system comprising proxy devices **112** and **114**, and rules **212** may be configured to cause rule gate **120** to route (or redirect) packets received from host **106** via one or more of interfaces **216**, **218**, or **220** and destined for host **142** (or a portion thereof (e.g., packets comprising data configured to establish a connection between hosts **106** and **142** and indicating the connection will be utilized to establish an encrypted communication session)) to host **142** via interface **226**. Additionally or alternatively, rules **212** may be configured to cause rule gate **120** to forward copies of (or mirror) packets received from host **106** via one or more of interfaces **216**, **218**, **220**, or **222** and destined for host **142** (or a portion thereof (e.g., packets comprising data configured to establish a connection between hosts **106** and **142** and indicating the connection will be utilized to establish an encrypted communication session)) to proxy device **112** via interface **226**.

At step #11, proxy devices **112** and **114** may exchange one or more parameters determined from the packets comprising the data configured to establish the connection between hosts **106** and **142**, for example, one or more network addresses in network-layer headers of the packets (e.g., network addresses of hosts **106** and **142**) or ports indicated by transport-layer headers in the packets (e.g., indicating the type of encrypted communication session the connection will be utilized to establish). Proxy device **112** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **112** and host **106** (e.g., a TCP:SYN-ACK handshake message) and, at step #12, may communicate the packets to host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #6 or #7), and one or more of log or drop the packets.

Similarly, proxy device **114** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **114** and host **142** (e.g., a TCP:SYN handshake message) and, at step #13, may communicate the packets to host **142**. Rule gate **128** may interface a communication link interfacing proxy device **114** and host **142**, and rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previ-

ously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps #6, #7, or #12), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device **112**, host **106** may generate packets comprising data configured to establish the connection between proxy device **112** and host **106** (e.g., a TCP:ACK handshake message) and, at step #14, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps #6, #7, #12, or #13), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device **114**, host **142** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:SYN-ACK handshake message) and, at step #15, may communicate the packets to proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s 6, 7, or 12-14), and one or more of log or drop the packets.

Responsive to receiving the packets from host **142**, proxy device **114** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:ACK handshake message) and, at step #16, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s 6, 7, or 12-15), and one or more of log or drop the packets.

Referring to FIG. 3B, proxy device **112** may receive the packets comprising data configured to establish the connection between proxy device **112** and host **106** communicated by host **106** in step #14, and connection **302** (e.g., a TCP connection) between proxy device **112** and host **106** may be established. Similarly, host **142** may receive the packets comprising data configured to establish the connection between proxy device **114** and host **142** communicated by proxy device **114** in step #16, and connection **304** (e.g., a TCP connection) between proxy device **114** and host **142** may be established.

At step #17, proxy device **112** and host **106** may communicate packets comprising data configured to establish encrypted communication session **306** (e.g., a SSL/TLS

session) between proxy device 112 and host 106 via connection 302. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-16), and one or more of log or drop the packets. Additionally or alternatively, rules 212 may be configured to cause rule gate 120 to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets. For example, in some embodiments, host 106 may comprise a client (e.g., web browser), host 142 may comprise a server (e.g., web server), the packets may comprise one or more handshake messages configured to establish session 306 that comprise unencrypted data including a domain name corresponding to the network-threat indicators, for example, a hello message generated by the client (e.g., including the domain name in the server name indication extension, or the like) or a certificate message generated by the server (e.g., including the domain name in one or more of the subject common name field or the extension subjectAltName (of type dNSName), or the like), and rules 212 may be configured to cause rule gate 120 to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the one or more handshake messages configured to establish session 306. In such embodiments, rules 212 may be configured to cause packet-filtering system 200 to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on the certificate message comprising other data (e.g., in addition to or in lieu of the domain name) corresponding to one or more of the network-threat indicators, for example, data indicating at least one of a serial number (or type thereof) indicated by rules 212, an issuer (or type thereof) indicated by rules 212, a validity time-range (or type thereof) indicated by rules 212, a key (or type thereof) indicated by rules 212, a digital signature (e.g., fingerprint) (or type thereof) indicated by rules 212, or a signing authority (or type thereof) indicated by rules 212.

Similarly, at step #18, proxy device 114 and host 142 may communicate packets comprising data configured to establish encrypted communication session 308 (e.g., a SSL/TLS session) between proxy device 114 and host 142 via connection 304, and rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-17) or the packets comprising one or more handshake messages configured to establish session 308 that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Host 106 may generate packets comprising data encrypted in accordance with one or more parameters of session 306

and, at step #19, may communicate the packets to proxy device 112 via session 306. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-18), and one or more of log (as indicated by the triangles over the line extending downward from rule gate 120) or drop the packets.

Proxy device 112 may receive the packets and decrypt the data in accordance with the parameters of session 306. The packets may comprise a request (e.g., a hypertext transfer protocol (HTTP) request), and proxy device 112 may comprise an ICAP client, which, at step #20, may communicate the packets to ICAP server 132. Rule gate 126 may interface a communication link interfacing proxy device 112 and ICAP server 132, and rules 212 may be configured to cause rule gate 126 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-19), and one or more of log or drop the packets.

ICAP server 132 may generate packets comprising data responsive to the request (e.g., a response, modified request, or the like) and, at step #21, may communicate the packets to proxy device 112. Rules 212 may be configured to cause rule gate 126 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-20), and one or more of log or drop the packets. Additionally or alternatively, rules 212 may be configured to cause rule gate 126 to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets, for example, the data responsive to the request (e.g., a modified request) may comprise data (e.g., a domain name, URI, or the like) corresponding to the network-threat indicators.

Proxy device 112 may generate packets (e.g., based on the data generated by ICAP server 132) and, at step #22, may communicate the packets to proxy device 114. Rule gate 124 may interface a communication link internal to the proxy system comprising proxy devices 112 and 114, and thus packets traversing the communication link may comprise unencrypted data (e.g., rule gate 124 may be “the man in the middle” of proxy devices 112 and 114), and rules 212 may be configured to cause rule gate 124 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-

11

threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-21), and one or more of log or drop the packets.

Additionally or alternatively, rules 212 may be configured to cause rule gate 124 to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets, for example, unencrypted data in the packets corresponding to one or more of the network-threat indicators. For example, in some embodiments, packet-filtering system 200 may implement one or more aspects of the technology described in U.S. patent application Ser. No. 13/795,822, filed Mar. 12, 2013, and entitled "FILTERING NETWORK DATA TRANSFERS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology, and rules 212 may be configured to cause rule gate 124 to one or more of identify the packets or determine that the packets comprise data corresponding to the one or more network-threat indicators based on the packets comprising one or more of a URI specified by rules 212, data indicating a protocol version specified by rules 212, data indicating a method specified by rules 212, data indicating a request specified by rules 212, or data indicating a command specified by rules 212. Additionally or alternatively, rules 212 may be configured to cause rule gate 124 to one or more of identify the packets or determine that the packets comprise data corresponding to the one or more network-threat indicators based on unencrypted data in the packets comprising a URI meeting or exceeding a threshold size specified by rules 212 (e.g., a URI likely being utilized to exfiltrate data).

Proxy device 114 may receive the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session 308 and, at step #23, may communicate the packets to host 142. Rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-22), and one or more of log or drop the packets.

Host 142 may generate one or more packets comprising data encrypted in accordance with one or more parameters of session 308 and, at step #24, may communicate the packets to proxy device 114. Rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-23), and one or more of log or drop the packets.

Proxy device 114 may receive the packets and generate one or more corresponding packets comprising unencrypted

12

data and, at step #25, may communicate the packets to proxy device 112. Rules 212 may be configured to cause rule gate 124 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-24), and one or more of log or drop the packets.

Proxy device 112 may receive the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session 306 and, at step #26, may communicate the packets to host 106. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-25), and one or more of log or drop the packets.

Host 106 may generate one or more packets comprising data encrypted in accordance with one or more parameters of session 306 and, at step #27, may communicate the packets toward proxy device 112. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-26), and one or more of log or drop the packets.

Proxy device 112 may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #28, may communicate the packets toward proxy device 114. Rules 212 may be configured to cause rule gate 124 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-27), and one or more of log or drop the packets.

Proxy device 114 may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session 308 and, at step #29, may communicate the packets toward host 142. Rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or

13

more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-28), and one or more of log or drop the packets.

Host 142 may generate one or more packets comprising data encrypted in accordance with one or more parameters of session 308 and, at step #30, may communicate the packets toward proxy device 114. Rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-29), and one or more of log or drop the packets.

Proxy device 114 may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #31, may communicate the packets toward proxy device 112. Rules 212 may be configured to cause rule gate 124 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-30), and one or more of log or drop the packets.

Proxy device 112 may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session 306 and, at step #32, may communicate the packets toward host 106. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-31), and one or more of log or drop the packets.

Referring to FIG. 3C, at step #33, rule gate 120 may one or more of update a console (or interface) associated with packet-filtering system 200 running on host 108 or receive one or more updates to rules 212 via the console. For example, the console may provide data regarding one or more threats to network 102 corresponding to the network-threat indicators, and rule gate 120 may update the console based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-32). In some embodiments, the console may provide data identifying network threats associated with one or more of hosts 106, 108, 110, 142, 144, or 146, and rule gate 120 may update data associated with one or more of hosts 106 or 142

14

based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-32).

At step #34, rule gate 120 may reconfigure rules 212 based on one or more of updates received via the console or data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-32). For example, packet-filtering system 200 may implement one or more aspects of the technology described in U.S. patent application Ser. No. 14/690,302, filed Apr. 17, 2015, and entitled "RULE-BASED NETWORK-THREAT DETECTION," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology, and rule gate 120 may reconfigure rules 212 based on one or more risk scores updated to reflect data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-32).

Host 106 may generate one or more packets comprising data encrypted in accordance with one or more parameters of session 306 and, at step #35, may communicate the packets toward proxy device 112. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, or 12-32), and one or more of log or drop the packets.

Proxy device 112 may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #36, may communicate the packets toward proxy device 114. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 124 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, or 35), and one or more of log or drop the packets.

Proxy device 114 may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session 308 and, at step #37, may communicate the packets toward host 142. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, 35, or 36), and one or more of log or drop the packets.

15

Host 142 may generate one or more packets comprising data encrypted in accordance with one or more parameters of session 308 and, at step #38, may communicate the packets toward proxy device 114. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, or 35-37), and one or more of log or drop the packets.

Proxy device 114 may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #39, may communicate the packets toward proxy device 112. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 124 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, or 35-38), and one or more of log or drop the packets.

Proxy device 112 may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session 306 and, at step #40, may communicate the packets toward host 106. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, or 35-39), and one or more of log or drop the packets.

Host 142 may generate one or more packets destined for one or more of hosts 106, 108, or 110 and, at step #41, may communicate the packets toward gateway 134. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, or 35-40), and one or more of log or drop the packets.

Host 108 may generate one or more packets and, at step #42, may communicate the packets to host 142. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may

16

be configured to cause rule gates 120 and 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, or 35-41), and one or more of log or drop the packets.

Host 106 may generate one or more packets destined for hosts 108, 142, 144, and 146 and, at step #43, may communicate the packets toward hosts 108, 142, 144, and 146. Rules 212 (e.g., one or more of rules 212 reconfigured in step #34) may be configured to cause rule gate 120 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6, 7, 12-32, or 35-42), and one or more of log or drop the packets.

Referring to FIG. 4A, step #s 1-5 substantially correspond to step #s 1-5 of FIG. 3A.

Host 106 (e.g., the web browser) may be configured to utilize web proxy 118 and responsive to the request, may generate packets comprising data configured to establish a connection between host 106 and web proxy 118 (e.g., a TCP:SYN handshake message) and, at step #6, may communicate the packets to web proxy 118. Rule gate 120 may interface a communication link interfacing host 106 and web proxy 118, and rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy 118) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

Responsive to receiving the packets from host 106, web proxy 118 may generate packets comprising data configured to establish the connection between host 106 and web proxy 118 (e.g., a TCP:SYN-ACK handshake message) and, at step #7, may communicate the packets to host 106. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy 118) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

Responsive to receiving the packets from web proxy 118, host 106 may generate packets comprising data configured to establish the connection between host 106 and web proxy 118 (e.g., a TCP:ACK handshake message) and, at step #8, may communicate the packets to web proxy 118. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy 118) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

Web proxy 118 may receive the packets from host 106, and connection 402 (e.g., a TCP connection) between host 106 and web proxy 118 may be established. Host 106 may

17

generate packets comprising a request (e.g., an HTTP CONNECT request), and, at step #9, may communicate the packets to web proxy 118 via connection 402. Rules 212 may be configured to cause rule gate 120 to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy 118) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, determine the packets comprise data corresponding to the network-threat indicators, for example, a domain name (e.g., FQDN) in the request, and one or more of log or drop the packets.

Web proxy 118 may generate a DNS query comprising the domain name and, at step #10, may communicate the DNS query toward DNS 130. The domain name included in the request may correspond to one or more of the network-threat indicators, and rules 212 may be configured to cause rule gate 126 to one or more of identify one or more packets comprising the DNS query, determine that the packets comprise the domain name corresponding to the network-threat indicators, and one or more of log or drop the packets. For example, the packets may comprise a network address of web proxy 118 (e.g., as a source address in their network-layer headers), and rule gate 126 may generate log data indicating the network address of web proxy 118. As depicted by step #10A, the packets may be communicated to DNS 130. In some embodiments, rules 212 may be configured to cause rule gate 126 to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching DNS 130, as depicted by step #10B.

DNS 130 may generate a reply to the DNS query and, at step #11, may communicate the reply toward web proxy 118. The reply may comprise the domain name corresponding to the network-threat indicators, and rules 212 may be configured to cause rule gate 126 to one or more of identify one or more packets comprising the reply, determine that the packets comprise the domain name corresponding to the network-threat indicators, and one or more of log or drop the packets. For example, the packets may comprise the network address of web proxy 118 (e.g., as a destination address in their network-layer headers), and rule gate 126 may generate log data indicating the network address of web proxy 118. Similarly, the domain name may correspond to host 142, the packets may comprise a network address of host 142 (e.g., DNS 130 may have resolved the domain name included in the query to the network address of host 142), and rule gate 126 may generate log data indicating the network address of host 142. As depicted by step #11A, the packets may be communicated to web proxy 118. In some embodiments, rules 212 may be configured to cause rule gate 126 to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching web proxy 118, as depicted by step #11B.

Web proxy 118 may generate one or more packets destined for host 142 comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between web proxy 118 and host 142 and, at step #12, may communicate the packets toward host 142. Rule gate 122 may interface a communication link interfacing web proxy 118 and host 142, and rules 212 may be configured to cause rule gate 122 to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets

18

with one or more of the packets comprising the request, the DNS query, or the reply to the DNS query based on data stored in logs 214 (e.g., the log data generated by rule gates 120 and 126 in one or more of step #s 6-11).

At step #13, rule gate 122 may route the packets comprising the data configured to establish the connection between web proxy 118 and host 142 to proxy device 112 and, at step #14, may communicate the packets to proxy device 112. For example, rules 212 may be configured to cause rule gate 122 to route the packets to proxy device 112 based on data in the packets, for example, one or more ports (e.g., port 443) indicated by transport-layer headers in the packets, indicating the connection between web proxy 118 and host 142 will be utilized to establish an encrypted communication session or tunnel (e.g., a session established in accordance with the transport layer security (TLS) protocol, secure sockets layer (SSL) protocol, secure shell (SSH) protocol, or the like).

Referring to FIG. 4B, at step #15, proxy devices 112 and 114 may exchange one or more parameters determined from the packets comprising the data configured to establish the connection between web proxy 118 and host 142, for example, one or more network addresses in network-layer headers of the packets (e.g., network addresses of web proxy 118 and host 142) or ports indicated by transport-layer headers in the packets (e.g., indicating the type of encrypted communication session the connection will be utilized to establish). Proxy device 112 may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device 112 and web proxy 118 (e.g., a TCP:SYN-ACK handshake message) and, at step #16, may communicate the packets to web proxy 118. Rules 212 may be configured to cause rule gate 122 to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the request, the DNS query, or the reply to the DNS query based on data stored in logs 214 (e.g., the log data generated by rule gates 120 and 126 in one or more of step #s 6-11).

Similarly, proxy device 114 may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device 114 and host 142 (e.g., a TCP:SYN handshake message) and, at step #17, may communicate the packets to host 142. Rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-11 or 16), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device 112, web proxy 118 may generate packets comprising data configured to establish the connection between proxy device 112 and web proxy 118 (e.g., a TCP:ACK handshake message) and, at step #18, may communicate the packets to proxy device 112. Rules 212 may be configured to cause rule gate 122 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example,

19

by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-11, 16, or 17), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device 114, host 142 may generate packets comprising data configured to establish the connection between proxy device 114 and host 142 (e.g., a TCP:SYN-ACK handshake message) and, at step #19, may communicate the packets to proxy device 114. Rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-11 or 16-18), and one or more of log or drop the packets.

Responsive to receiving the packets from host 142, proxy device 114 may generate packets comprising data configured to establish the connection between proxy device 114 and host 142 (e.g., a TCP:ACK handshake message) and, at step #20, may communicate the packets to host 142. Rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-11 or 16-19), and one or more of log or drop the packets.

Proxy device 112 may receive the packets comprising data configured to establish the connection between proxy device 112 and web proxy 118 communicated by web proxy 118 in step #18, and connection 404 (e.g., a TCP connection) between proxy device 112 and web proxy 118 may be established. Similarly, host 142 may receive the packets comprising data configured to establish the connection between proxy device 114 and host 142 communicated by proxy device 114 in step #20, and connection 406 (e.g., a TCP connection) between proxy device 114 and host 142 may be established.

At step #21, proxy device 112 and host 106 may communicate packets comprising data configured to establish encrypted communication session 408 (e.g., a SSL/TLS session) between proxy device 112 and host 106 via connections 402 and 404. Rules 212 may be configured to cause one or more of rule gates 120 or 122 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-11 or 16-20) or the packets comprising one or more handshake messages configured to establish session 408 that comprise unencrypted data (e.g.,

20

including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Similarly, at step #22, proxy device 114 and host 142 may communicate packets comprising data configured to establish encrypted communication session 410 (e.g., a SSL/TLS session) between proxy device 114 and host 142 via connection 406, and rules 212 may be configured to cause rule gate 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-11 or 16-21) or the packets comprising one or more handshake messages configured to establish session 410 that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Referring to FIGS. 4B-C, step #s 23-47 substantially correspond to step #s 19-43 of FIGS. 3B-C; however, rules 212 may be configured to cause one or more of rule gates 120 or 122 to one or more of identify, drop, or log the packets communicated in one or more of step #s 23, 30, 31, 36, 39, or 44 of FIGS. 4B-C.

Referring to FIG. 5A, step #s 1-7 substantially correspond to step #s 1-7 of FIG. 3A.

Host 106 may generate one or more packets destined for host 142 comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between hosts 106 and 142 and, at step #8, may communicate the packets to host 142. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs 214 (e.g., the log data generated by rule gate 126 in one or more of steps #6 or #7).

Responsive to receiving the packets from host 106, host 142 may generate packets comprising data configured to establish the connection between hosts 106 and 142 (e.g., a TCP:SYN-ACK handshake message) and, at step #9, may communicate the packets to host 106. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs 214 (e.g., the log data generated by rule gate 126 in one or more of steps #6 or #7).

Responsive to receiving the packets from host 142, host 106 may generate packets comprising data configured to establish the connection between hosts 106 and 142 (e.g., a TCP:ACK handshake message) and, at step #10, may communicate the packets to host 142. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating

21

the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs 214 (e.g., the log data generated by rule gate 126 in one or more of steps #6 or #7).

Host 142 may receive the packets comprising data configured to establish the connection between hosts 106 and 142 communicated by host 106 in step #10, and connection 502 (e.g., a TCP connection) between hosts 106 and 142 may be established.

At step #11, hosts 106 and 142 may communicate packets comprising data configured to establish encrypted communication session 504 (e.g., a SSL/TLS session) between hosts 106 and 142 via connection 502. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-10) or the packets comprising one or more handshake messages configured to establish session 504 that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Host 106 may generate packets comprising data encrypted in accordance with one or more parameters of session 504 and, at step #12, may communicate the packets to host 142. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-11), and one or more of log or drop the packets.

Host 142 may generate packets comprising data encrypted in accordance with one or more parameters of session 504 and, at step #13, may communicate the packets to host 106. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-12), and one or more of log or drop the packets.

Host 106 may generate packets comprising data encrypted in accordance with one or more parameters of session 504 and, at step #14, may communicate the packets toward host 142. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log

22

data generated by packet-filtering system 200 in one or more of step #s 6-13), and one or more of log or drop the packets.

Host 142 may generate packets comprising data encrypted in accordance with one or more parameters of session 504 and, at step #15, may communicate the packets toward host 106. Rules 212 may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-14), and one or more of log or drop the packets.

Referring to FIG. 5B, steps #16 and #17 substantially correspond to steps #33 and #34 of FIG. 3C.

Host 106 may generate packets comprising data encrypted in accordance with one or more parameters of session 504 and, at step #18, may communicate the packets toward host 142. Rules 212 (e.g., one or more of rules 212 reconfigured in step #17) may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-15), and one or more of log or drop the packets.

Host 142 may generate packets comprising data encrypted in accordance with one or more parameters of session 504 and, at step #19, may communicate the packets toward host 106. Rules 212 (e.g., one or more of rules 212 reconfigured in step #17) may be configured to cause one or more of rule gates 120 or 128 to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system 200 to comprise data corresponding to the network-threat indicators based on data stored in logs 214 (e.g., log data generated by packet-filtering system 200 in one or more of step #s 6-15 and 18), and one or more of log or drop the packets.

Step #s 20-22 substantially correspond to step #s 41-43 of FIG. 3C.

Referring to FIG. 6A, step #s 1-11 substantially correspond to step #s 1-11 of FIG. 4A.

Web proxy 118 may generate one or more packets destined for host 142 comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between web proxy 118 and host 142 and, at step #12, may communicate the packets to host 142. Rules 212 may be configured to cause one or more of rule gates 122 or 128 to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply

## 23

to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#10** or **#11**).

Responsive to receiving the packets from web proxy **118**, host **142** may generate packets comprising data configured to establish the connection between web proxy **118** and host **142** (e.g., a TCP:SYN-ACK handshake message) and, at step **#13**, may communicate the packets to web proxy **118**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#10** or **#11**).

Responsive to receiving the packets from host **142**, web proxy **118** may generate packets comprising data configured to establish the connection between web proxy **118** and host **142** (e.g., a TCP:ACK handshake message) and, at step **#14**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#10** or **#11**).

Referring to FIG. **6B**, host **142** may receive the packets comprising data configured to establish the connection between web proxy **118** and host **142** communicated by web proxy **118** in step **#14**, and connection **604** (e.g., a TCP connection) between web proxy **118** and host **142** may be established.

At step **#15**, hosts **106** and **142** may communicate packets comprising data configured to establish encrypted communication session **606** (e.g., a SSL/TLS session) between hosts **106** and **142** via connections **602** and **604**. Rules **212** may be configured to cause one or more of rule gates **120**, **122**, or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-15**) or the packets comprising one or more handshake messages configured to establish session **606** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Step **#s 16-26** substantially correspond to step **#s 12-22** of FIGS. **5A-B**; however, rules **212** may be configured to cause one or more of rule gates **120**, **122**, or **128** to one or more of identify, drop, or log the packets communicated in one or more of step **#s 16-19**, **22**, or **23** of FIG. **6B**.

FIG. **7** depicts an illustrative method for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to FIG. **7**, in step **702**, a packet-filtering system may receive data indicating network-threat indicators. For

## 24

example, packet-filtering system **200** may receive packet-filtering rules generated by rule provides **138** based on network-threat indicators provided by threat-intelligence providers **140**. In step **704**, the packet-filtering system may configure packet-filtering rules in accordance with which it is configured to filter packets. For example, packet-filtering system **200** may configure rules **212**.

In step **706**, the packet-filtering system may identify packets comprising unencrypted data. For example, packet-filtering system **200** may identify packets comprising a DNS query, a reply to a DNS query, or a handshake message configured to establish an encrypted communication session. In step **708**, the packet-filtering system may identify packets comprising encrypted data. For example, packet-filtering system **200** may identify packets encrypted in accordance with one or more parameters of sessions **306**, **308**, **408**, **410**, **504**, or **606**.

In step **710**, the packet-filtering system may determine based on a portion of the unencrypted data corresponding to the network-threat indicators that the packets comprising encrypted data correspond to the network-threat indicators. For example, packet-filtering system **200** may determine that a domain name included in the DNS query, the reply to the DNS query, or the handshake message corresponds to the network-threat indicators, and packet-filtering system **200** may determine that one or more of the packets encrypted in accordance with the parameters of sessions **306**, **308**, **408**, **410**, **504**, or **606** correlate to one or more packets comprising the DNS query, the reply to the DNS query, or the one or more handshake messages.

The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer-executable instructions and computer-usable data described herein.

Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, system, apparatus, or one or more computer-readable media storing computer-executable instructions. Accordingly, aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

As described herein, the various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like).

25

Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order and that one or more illustrated steps may be optional. Any and all features in the following claims may be combined or rearranged in any way possible.

What is claimed is:

1. A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

2. The method of claim 1, wherein:

the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query, the method further comprising:

determining that the at least one of the DNS query or the reply to the DNS query comprises the domain name identified as the network threat.

3. The method of claim 2, wherein the portion of the unencrypted data comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

4. The method of claim 2, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets

26

comprising the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

5. The method of claim 4, wherein the one or more network addresses comprise a network address of a web proxy that generated the DNS query in response to a request received from a host, the method further comprising:

identifying one or more packets comprising the request.

6. The method of claim 1, wherein one or more packets, of the packets comprising unencrypted data, comprise data configured to establish an encrypted communication session between a first host and a second host, the method further comprising:

routing the one or more packets comprising data configured to establish the encrypted communication session between the first host and the second host to the proxy system.

7. The method of claim 6, the method further comprising: routing the one or more packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the domain name identified as the network threat.

8. The method of claim 6, wherein:

the plurality of packet-filtering rules indicate:

one or more network addresses for which encrypted communications are to be established via the proxy system, and

one or more network addresses for which encrypted communications are to not be established via the proxy system, the method further comprising:

routing the one or more packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications are to be established via the proxy system.

9. The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

redirecting packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

10. The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

forwarding copies of packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

27

11. The method of claim 6, the method further comprising:

identifying, via a communication link interfacing the first host and the proxy system, the packets comprising encrypted data; and

identifying, via an internal communication link of the proxy system, packets corresponding to the packets comprising encrypted data.

12. The method of claim 11, the method further comprising: identifying, via a communication link interfacing the proxy system and the second host, packets generated by the proxy system based on the packets corresponding to the packets comprising encrypted data.

13. The method of claim 6, the method further comprising:

generating, by the proxy system, one or more packets based on the filtered packets, comprising encrypted data, routed to the proxy system by the packet-filtering system;

responsive to determining that one or more packets generated by the proxy system correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of:

dropping the one or more packets generated by the proxy system;

logging the one or more packets generated by the proxy system;

dropping one or more other packets generated by the proxy system;

logging one or more other packets generated by the proxy system;

dropping one or more other packets comprising encrypted data; or

logging one or more other packets comprising encrypted data.

14. The method of claim 13, wherein the determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules comprises determining that the one or more packets generated by the proxy system comprise at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules.

15. The method of claim 13, wherein the determining comprises determining that the one or more packets generated by the proxy system comprise a uniform resource identifier (URI) meeting a threshold size specified by the plurality of packet-filtering rules.

16. The method of claim 6, the method further comprising: identifying, via a communication link interfacing the proxy system and an Internet content adaptation protocol (ICAP) server, one or more packets comprising at least one of an ICAP request, a response generated by the ICAP server, or a modified request generated by the ICAP server.

17. The method of claim 1, wherein the packets comprising encrypted data comprise packets received from a first host and destined for a second host, the method further comprising at least one of dropping or logging packets other than the packets comprising encrypted data based on a determination that the packets other than the packets comprising encrypted data were at least one of received from the second host or destined for the first host.

28

18. The method of claim 1, wherein:

the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:

determining that the one or more handshake messages comprise the domain name identified as the network threat.

19. The method of claim 18, the method further comprising: responsive to determining that the one or more handshake messages comprise the domain name identified as the network threat, at least one of dropping or logging the packets comprising encrypted data.

20. The method of claim 18, wherein:

the one or more handshake messages comprise at least one of a hello message generated by the client or a certificate message generated by the server; and

the determining that the one or more handshake messages comprise the domain name identified as the network threat comprises determining the at least one of the hello message generated by the client or the certificate message generated by the server comprises the domain name identified as the network threat.

21. The method of claim 18, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the one or more handshake messages, the method further comprising

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

22. The method of claim 21, wherein the one or more network addresses comprise a network address of the server and a network address of a web proxy, the method further comprising:

identifying one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and

determining that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.

23. The method of claim 1, wherein the packets comprising unencrypted data comprise a certificate message for an encrypted communication session, the method further comprising:

at least one of dropping or logging one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules.

24. A packet-filtering system comprising:

at least one hardware processor; and  
memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

29

identify packets comprising unencrypted data;  
 identify packets comprising encrypted data;  
 determine, based on a portion of the unencrypted data  
 corresponding to one or more network-threat indi-  
 cators of the plurality of network-threat indicators, 5  
 packets comprising encrypted data that corresponds  
 to the one or more network-threat indicators;  
 filter, based on at least one of a uniform resource  
 identifier (URI) specified by a plurality of packet-  
 filtering rules, data indicating a protocol version 10  
 specified by the plurality of packet-filtering rules,  
 data indicating a method specified by the plurality of  
 packet-filtering rules, data indicating a request speci-  
 fied by the plurality of packet-filtering rules, or data 15  
 indicating a command specified by the plurality of  
 packet-filtering rules:  
 packets comprising the portion of the unencrypted  
 data corresponding to one or more network-threat  
 indicators of the plurality of network-threat indi- 20  
 cators; and  
 the determined packets comprising the encrypted  
 data that corresponds to the one or more network-  
 threat indicators; and  
 route, by the packet-filtering system, filtered packets to 25  
 a proxy system based on a determination that the  
 filtered packets comprise data that corresponds to the  
 one or more network-threat indicators.

25. One or more non-transitory computer-readable media  
 comprising instructions that when executed by at least one 30  
 hardware processor of a packet-filtering system cause the  
 packet-filtering system to:

30

receive data indicating a plurality of network-threat indi-  
 cators, wherein at least one of the plurality of network-  
 threat indicators comprise a domain name identified as  
 a network threat;  
 identify packets comprising unencrypted data;  
 identify packets comprising encrypted data;  
 determine, based on a portion of the unencrypted data  
 corresponding to one or more network-threat indicators  
 of the plurality of network-threat indicators, packets  
 comprising encrypted data that corresponds to the one  
 or more network-threat indicators;  
 filter, by the packet-filtering system and based on at least  
 one of a uniform resource identifier (URI) specified by  
 a plurality of packet-filtering rules indicating one or  
 more of the plurality of network-threat indicators, data  
 indicating a protocol version specified by the plurality  
 of packet-filtering rules, data indicating a method  
 specified by the plurality of packet-filtering rules, data  
 indicating a request specified by the plurality of packet-  
 filtering rules, or data indicating a command specified  
 by the plurality of packet-filtering rules:  
 packets comprising the portion of the unencrypted data  
 corresponding to one or more network-threat indicators  
 of the plurality of network-threat indicators; and  
 the determined packets comprising the encrypted data that  
 corresponds to the one or more network-threat indica-  
 tors; and  
 route, by the packet-filtering system, filtered packets to a  
 proxy system based on a determination that the filtered  
 packets comprise data that corresponds to the one or  
 more network-threat indicators.

\* \* \* \* \*