UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
TEXARKANA DIVISION

SABLE NETWORKS, INC. AND SABLE IP, LLC,

Plaintiffs,

v.

FORTINET, INC. AND MASERGY COMMUNICATIONS, INC.,

Defendants.

Civil Action No._____

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Sable Networks, Inc. and Sable IP, LLC (collectively, "Sable" or "Plaintiffs") bring this action and make the following allegations of patent infringement relating to U.S. Patent Nos.: 6,954,431 (the "'431 patent"); 8,243,593 (the "'593 patent"); 8,817,790 (the "'790 patent"); and 9,774,501 (the "'591 patent") (collectively, the "patents-in-suit"). Defendants Fortinet, Inc. ("Fortinet") and Masergy Communications, Inc. ("Masergy") (collectively, "Defendants") infringe each of the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. The patents-in-suit arise from technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the internet.[1] The patents relate to technologies for efficiently managing the flow of data packets over routers and switch devices. Dr. Roberts and engineers at Caspian Networks, Inc. and later Sable Networks, Inc. developed these technologies to address the

[1] Chris Woodford, THE INTERNET: A HISTORICAL ENCYCLOPEDIA VOLUME 2 at 204 (2005) ("Widely regarded as one of the founding fathers of the Internet, Lawrence Roberts was the primary architect of ARPANET, the predecessor of the Internet.").

increasing amount of data sent over computer networks.

2. The allegations of patent infringement contained herein arise out of the same series of transactions or occurrences relating to the making, using, selling, offering for sale, and/or importing within the United States, the products accused of infringing the patents-in-suit—the Masergy SD-WAN Solutions,[2] which include at least the following product offerings: Masergy SD-WAN Secure,[3] Masergy Co-Managed SD-WAN,[4] Masergy Managed SD-WAN Secure OTT,[5] Masergy SD-WAN Home,[6] Masergy SD-WAN Branch solutions,[7] Masergy Secure Access

[2] *See e.g.*, *Berkshire Partners Completes Acquisition of Masergy*, BERKSHIRE PARTNERS PRESS RELEASE (December 21, 2016) ("Masergy owns and operates the largest independent Software Defined Platform in the world, delivering hybrid networking, managed security and cloud communication solutions to global enterprises.").

[3] *Answering Partner FAQs On Managed SD-WAN,* MASERGY DOCUMENTATION (2020) ("Masergy SD-WAN Secure solutions are powered by Fortinet to provide customers with integrated security features such as a next-generation firewall").

[4] *Masergy Expands Its SD-WAN Portfolio Offering the Broadest Choice, Flexibility and Built-In SASE,* MASERGY PRESS RELEASE (July 21, 2020) ("Co-managed solutions: Leveraging the SD-WAN Orchestrator, clients can customize their configurations and make changes while Masergy simultaneously monitors and reports on performance.").

[5] *Masergy Managed SD-WAN Secure OTT*: *Internet Strategies Built For Security and Choice,* MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/managed-sd-wan-secure-ott ("How Masergy's SD-WAN Secure OTT works: Masergy creates an overlay network on top of any public or private network and sends encrypted application traffic via IPsec tunnels to Fortinet-powered endpoints over the public internet ('over the top') for your secure, agile, and scalable corporate network.").

[6] Andy Patrizio, *Masergy teams with Fortinet for at-home SD-WAN*, NETWORKWORLD.COM ARTICLE (October 19, 2020) *available at*: https://www.networkworld.com/article/3586177/masergy-teams-with-fortinet-for-at-home-sd-wan.html ("The SD-WAN Secure Home offering utilizes a lightweight Fortinet Secure SD-WAN device for connectivity and improved application performance over a home Internet connection. It also includes built-in next-generation firewall and routing, direct connections to an ecosystem of cloud services").

[7] *Extending secure SD-WAN to secure SD-Branch*: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge ("Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.").

Service Edge solutions (SASE),[8] and Masergy Secure Web Gateway solutions[9] (collectively, the "Masergy-Fortinet Products"). The Masergy-Fortinet Products contain Fortinet-provided hardware, including: FortiGate Next-Generation Firewalls, Fortinet Application-Specific Integrated Circuits (ASIC), and Fortinet SD-WAN.

Q: What security features do Masergy SD-WAN Secure solutions offer?
A: Masergy SD-WAN Secure solutions are powered by Fortinet to provide customers with integrated security features such as a next-generation firewall, encrypted tunneling over the public internet, and unified threat management capabilities at every site. Customers can add the following cybersecurity features to their SD-WAN Secure deployments:

- **SD-WAN with Unified Threat Management (UTM):**
  Masergy SD-WAN Secure solution with added security visibility around intrusion detection, malware, and application control in the Masergy customer portal.
- **SD-WAN with Threat Monitoring & Response (TMR):**
  Enhanced security for SD-WAN that layers UTM plus global 24/7 live monitoring and incident response against suspicious events on your network.
- **SD-WAN with Managed Security Services (MSS):**
  Full managed detection and response cybersecurity solution for Masergy SD-WAN Secure deployments leveraging patented machine-learning network behavioral analytics and global 24/7 live threat hunting from tenured security analysts.

Answering Partner FAQs On Managed SD-WAN, MASERGY DOCUMENTATION at 3 (2020) (emphasis added).

3. The Masergy-Fortinet Products are based on a partnership between Fortinet and Masergy and have been described in Masergy's documentation as the "Masergy-Fortinet offering." The following excerpt from an October 2020 article from the Masergy website describes the Masergy-Fortinet Products as the result of "Masergy and Fortinet hav[ing] partnered together."

> With network and security solutions each recognized by Gartner, Fortinet and Masergy have partnered together to compete in the budding new Secure Access Service Edge (SASE) industry with converged offerings that are differentiated in

[8] *SASE from Fortinet & Masergy*: *Converging best-of-breed network and security solutions recognized by Gartner,* MASERGY BLOG POSTING (October 6, 2020), *available at*: https://www.masergy.com/blog/sase-from-fortinet-masergy-converging-best-of-breed-network-and-security-solutions-recognized-by-gartner ("Investors seeking out SASE solutions are demanding best-of-breed technologies converged into one solution, and it's here where the Masergy-Fortinet offering stands above the rest.").

[9] *Masergy Secure Web Gateway*, MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/sase/secure-web-gateway ("Masergy's secure web gateway solution is powered by Fortinet . . . Fortinet SWGs go beyond standard web proxies to keep enterprise networks safe from malicious internet traffic, preventing threats from entering the network and causing an infection or intrusion.").

> the market. . . . Investors seeking out SASE solutions are demanding best-of-breed technologies converged into one solution, and it's here where the Masergy-Fortinet offering stands above the rest. We are uniquely positioned to compete in this new market with Gartner-recognized offerings that come in a single, seamless SASE solution delivered as a fully managed cloud service.

SASE from Fortinet & Masergy: *Converging best-of-breed network and security solutions recognized by Gartner,* MASERGY BLOG POSTING (October 6, 2020), *available at*: https://www.masergy.com/blog/sase-from-fortinet-masergy-converging-best-of-breed-network-and-security-solutions-recognized-by-gartner (emphasis added).

4. Fortinet documentation has described the Masergy-Fortinet Products as the result of Fortinet and Masergy "team[ing] up to create a range of differentiated and fully managed SD-WAN offerings."

> The growing pressures of digital innovation (DI) have spurred the rapid adoption of software-defined wide area networking (SD-WAN). But SD-WAN must be secured. That is why Fortinet and Masergy have teamed up to create a range of differentiated and fully managed SD-WAN offerings, encompassing Fortinet's advanced technologies and Masergy's end-to-end security services.

Fortinet Customer Profile: *Masergy*, FORTINET.COM WEBSITE (last visited December 2020), *available at*: https://www.fortinet.com/customers/masergy (emphasis added).

5. Defendants' documentation identifies that the accused Masergy-Fortinet Products enable protecting network traffic at a packet level, and the FortiGate secure web gateway protects IP traffic at an application level "both in the cloud and on-premise."

> Best-in-Class Secure Web Gateway from Fortinet: Giving clients the advantage of more SASE capabilities from trusted brands, Masergy has standardized its cloud platform around Fortinet's best-in-class secure web gateway (SWG) solution. Fortinet is named a Leader in Gartner Inc.'s September 2020 Magic Quadrant for WAN Edge Infrastructure3 report. Fortinet firewalls protect network traffic at a packet level, and the FortiGate SWG protects IP traffic at an application level—both in the cloud and on-premise. In addition to SWG, cloud-based application control and content filters include granular per-app and per-user visibility with Masergy's Identity-Based WAN Analytics. And as a managed security services provider, Masergy also offers a full complement of cybersecurity solutions—from threat monitoring and endpoint detection and response, all the way up to full 24/7 management.

Masergy Strengthens Its SD-WAN Secure Solution with Deeper SASE Capabilities, MASERGY PRESS RELEASE (November 16, 2020), *available at*: https://www.masergy.com/press-release/masergy-strengthens-its-sd-wan-secure-solution-with-deeper-sase-capabilities (emphasis added).

6. Fortinet's FortiGate Next-Generation Firewalls, Fortinet Application-Specific Integrated Circuits (ASIC), and Fortinet SD-WAN products are specifically developed, marketed, licensed and distributed by Fortinet to be used in SD-WAN offerings such as Masergy's SD-WAN solution.

> You'll get the broadest SD-WAN options, SASE-based security at the core, controls to reconfigure services on the fly, and unprecedented Service Level Agreements (SLAs) delivering performance perfection. With the only pure software-defined edge network, Masergy is your partner for reliability and business continuity. Fortinet® edge devices and built-in firewalls on premise or in the cloud along with a menu of managed security services offer a holistic approach for the best end-to-end management— enabling employees to work from anywhere.

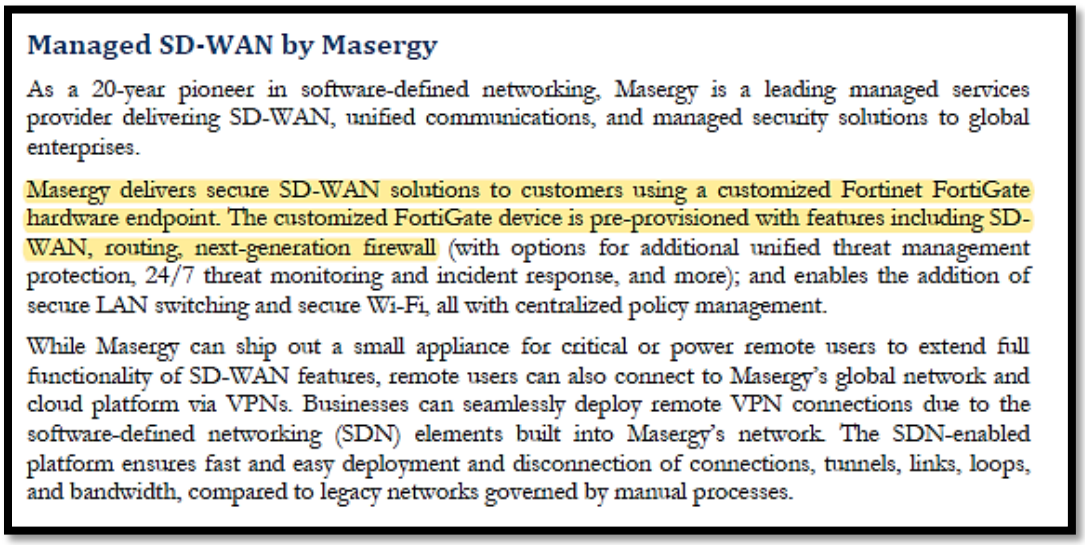
Masergy SD-WAN Secure, MASERGY SOLUTIONS BRIEF at 1 (2020) (emphasis added).

7. Fortinet is liable for induced and contributory infringement of the Asserted Patents based on forming a joint enterprise with Fortinet with respect to building and distributing the FortiGate Next-Generation Firewalls, Fortinet Application-Specific Integrated Circuits (ASIC), and Fortinet SD-WAN products, which are specifically built to perform the infringing functionality.

> Fortinet and Masergy are strategic partners, and together we have built a differentiated and fully managed SD-WAN offering, helping organizations truly transform the WAN edge with a security-driven approach that encompasses advanced technologies and end-to-end security services. Masergy is in a unique position to deliver security services and software-defined network services built on Fortinet's secure SD-WAN solution.

Fortinet & Masergy: *The security-driven approach to SD-WAN*, MASERGY BLOG POSTING (January 16, 2020) *available at*: https://www.masergy.com/blog/fortinet-masergy-the-security-driven-approach-to-sd-wan (emphasis added).

8. Fortinet's relationship with Masergy goes beyond simply selling components to Masergy. Because the selection and incorporation process for technology in the Masergy SD-WAN offerings is a lengthy one, Fortinet works closely with Masergy to "define" and "design" Fortinet products placed in the Masergy SD-WAN offerings.



Managed SD-WAN by Masergy

As a 20-year pioneer in software-defined networking, Masergy is a leading managed services provider delivering SD-WAN, unified communications, and managed security solutions to global enterprises.

Masergy delivers secure SD-WAN solutions to customers using a customized Fortinet FortiGate hardware endpoint. The customized FortiGate device is pre-provisioned with features including SD-WAN, routing, next-generation firewall (with options for additional unified threat management protection, 24/7 threat monitoring and incident response, and more); and enables the addition of secure LAN switching and secure Wi-Fi, all with centralized policy management.

While Masergy can ship out a small appliance for critical or power remote users to extend full functionality of SD-WAN features, remote users can also connect to Masergy's global network and cloud platform via VPNs. Businesses can seamlessly deploy remote VPN connections due to the software-defined networking (SDN) elements built into Masergy's network. The SDN-enabled platform ensures fast and easy deployment and disconnection of connections, tunnels, links, loops, and bandwidth, compared to legacy networks governed by manual processes.

Roopa Honnachari, *COVID-19 Highlights the Business Case for Extending SD-WAN to Remote Workers,* BUSINESS COMMUNICATION SERVICES (BCS) VOL. 14 NO. 1 at 8 (May 2020) (emphasis added).

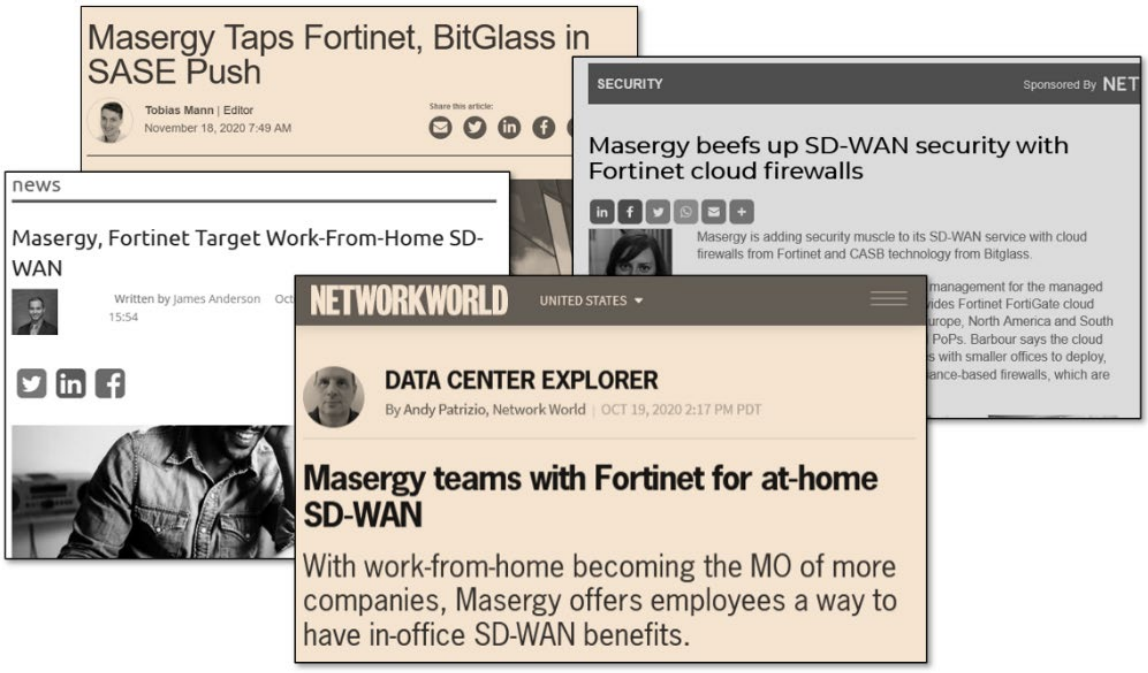
9. Masergy and Fortinet share a community of pecuniary interests in the development and distribution of the Masergy-Fortinet Products. For example, upon information and belief, there are indemnification and revenue provisions, as set forth in the agreements between the two companies. Both Masergy and Fortinet derive financial benefit from the development and distribution of the Masergy-Fortinet Products.

10. Fortinet-provided components contained in the Masergy-Fortinet Products have been identified by Fortinet and Masergy as "powering" the Masergy-Fortinet Products.

> Masergy's secure web gateway solution is powered by Fortinet, the Leader in the Gartner Magic Quadrant for WAN Edge Infrastructure. Fortinet SWGs go beyond standard web proxies to keep enterprise networks safe from malicious internet traffic, preventing threats from entering the network and causing an infection or intrusion.

Masergy Secure Web Gateway, MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/sase/secure-web-gateway (emphasis added).

11. Masergy and Fortinet have represented to the public that they have "teamed up" and are jointly "targeting" the SD-WAN market through the Masergy-Fortinet Products.



Tobias Mann, *Masergy Taps Fortinet, BitGlass in SASE Push,* SDXCENTRAL.COM ARTICLE (November 18, 2020); Kelsey Kusterer Ziser, *Masergy beefs up SD-WAN security with Fortinet cloud firewalls*, LIGHTREADING.COM WEBSITE (November 16, 2020); Andy Patrizio, *Masergy teams with Fortinet for at-home SD-WAN*, NETWORKWORLD.COM ARTICLE (October 19, 2020); James Anderson, *Masergy, Fortinet Target Work-From-Home SD-WAN*, CHANNEL PARTNERS.COM ARTICLE (October 13, 2020).

12. Masergy's SD-WAN offerings rely on products provided by Fortinet. In November 2020, Masergy announced that it was incorporating Fortinet FortiGate firewalls into ***all*** of Masergy's software-defined networking over wide area network (SD-WAN) points of presence (PoPs). *Masergy Strengthens Its SD-WAN Secure Solution with Deeper SASE Capabilities*, MASERGY PRESS RELEASE (November 16, 2020).

13. Fortinet conditions both the manner and timing of the performance of steps by Masergy in building and distributing the Masergy-Fortinet Products, and is thus liable for indirect infringement of the patents-in-suit.

> Unlike other providers, our Managed SD-WAN solutions enable you to leverage SD-WAN at some locations without having to deploy it everywhere in a "mix and match" WAN design approach. Masergy SD-WAN endpoint hardware is provided by our partners at Fortinet with an embedded router, firewall, and unified threat management (UTM) capabilities. Combined with our managed software-defined

> network backbone, these features enable companies to install secure Managed SD-WAN connections quickly and safely on their network edge that extends to both public and private cloud assets.

Masergy: *Your SD-WAN questions answered,* MASERGY WEBSITE (last visited December 2020); *available at*: https://www.masergy.com/faq/managed-sd-wan (emphasis added).

14. The inclusion of the Fortinet components in the Masergy SD-WAN offering has been described as "adding security muscle" to the Masergy SD-WAN product offerings. Further, Masergy hosts and maintains the Masergy-Fortinet Products at data centers and other points-of-presence.

> Masergy is adding security muscle to its SD-WAN service with cloud firewalls from Fortinet and CASB technology from Bitglass. Jay Barbour, director of security product management for the managed service provider, says Masergy now provides Fortinet FortiGate cloud firewalls across Africa, Asia, Australia, Europe, North America and South America, as well as throughout its global PoPs. Barbour says the cloud firewall is easier and faster for companies with smaller offices to deploy.

Kelsey Kusterer Ziser, *Masergy beefs up SD-WAN security with Fortinet cloud firewalls*, LIGHTREADING.COM WEBSITE (November 16, 2020), *available at*: https://www.lightreading.com/security/masergy-beefs-up-sd-wan-security-with-fortinet-cloud-firewalls/d/d-id/765470.

15. All of the accused Masergy-Fortinet Products contain Fortinet SD-WAN components. A February 2020 press release from Fortinet quotes Masergy's Executive Vice President as stating, "Built on Fortinet's Secure SD-WAN, Masergy's Managed SD-WAN solution gives clients software-defined network services and three tiered options for managed security services. It's a winning combination that resonates with global enterprises needing cloud application performance, 24/7 threat monitoring, as well as incident response." *Fortinet Drives Channel Business Opportunities with Secure SD-WAN*, FORTINET PRESS RELEASE (February 5, 2020).

16. Masergy and Fortinet marketing materials reflect the integral role Fortinet devices play in Masergy's SD-WAN offerings. Masergy, in a recent webcast, described that the inclusion of Fortinet components in the Masergy SD-WAN offerings "allows us to integrate a full UTM

suite or unified threat management suite" and "deliver an SD-WAN solution that has a security practice."

CNSG ProviderSMART with John Marinucci of Masergy, CNSG AN APPSMART COMPANY YOUTUBE CHANNEL AT 13:40-14:02 (August 13, 2020), *available at*: https://www.youtube.com/watch?v=jYFnX-GK7qg ("The company we strategically work with is a company called Fortinet who you know I think most people know has a very strong reputation in the security space. So that chassis allows us to integrate a full UTM suite or unified threat management suite but also take the logging event from that point it up to a cloud and have our software monitor a lot of events so when I now can deliver an SD-Wan solution that has a security practice.").

17. Fortinet has hosted joint presentations with Masergy that highlight the inclusion of Fortinet components in the Masergy-Fortinet Products. The following excerpts from an April 2020 webcast hosted by Fortinet detailed the inclusion and value of Fortinet components in the Masergy SD-WAN offering.

Enabling Enterprises with Secure, Agile and Intelligent Managed SD-WAN, MASERGY-FORTINET PARTNER WEBCAST (April 29, 2020), *available at*: https://www.fortinet.com/resources-campaign/network.

BACKGROUND OF SABLE NETWORKS' GROUNDBREAKING INNOVATIONS

18. Sable Networks is a maker of networking equipment based on technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the Internet. Dr. Roberts is best known for his work as the Chief Scientist of the Advanced Research Projects Agency (ARPA) where he designed and oversaw the implementation of ARPANET, the precursor to the internet. Dr. Roberts' work on ARPANET played a key role in the development of digital network transmission technologies.[10] Initially, ARPANET was used primarily to send electronic mail and Dr. Roberts developed the first program for reading and sending electronic messages.

[10] Katie Hafner, *Lawrence Roberts, Who Helped Design Internet's Precursor,* N.Y. TIMES at A2 (December 31, 2018) ("Dr. Roberts was considered the decisive force behind packet switching, the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.").

Keenan Mayo and Peter Newcomb, *How The Web Was Won*, VANITY FAIR at 96-97 (January 7, 2009); *One of the Engineers Who Invented the Internet Wants to Build A Radical new Router,* IEEE SPECTRUM MAGAZINE (July 2009); Katie Hafner, *Billions Served Daily, and Counting*, N.Y. TIMES at G1 (December 6, 2001)("Lawrence Roberts, who was then a manager at the Advanced Research Projects Agency's Information Processing Techniques Office, solved that problem after his boss began complaining about the volume of e-mail piling up in his in box. In 1972, Dr. Roberts produced the first e-mail manager, called RD, which included a filing system, as well as a Delete function.").

19. Dr. Roberts' work on ARPANET played a key role in the development of packet switching networks. Packet switching is a digital network transmission process in which data is broken into parts which are sent independently and reassembled at a destination. Electronic messages sent over the ARPANET were broken up into packets then routed over a network to a destination. "In designing the ARPANET, Roberts expanded on the work he'd done at MIT, using those tiny data packets to send information from place to place."[11] Packet switching has become the primary technology for data communications over computer networks.

[11] Code Metz, *Larry Roberts Calls Himself the Founder of The Internet. Who Are You To Argue*, WIRED MAGAZINE (September 24, 2012); John C. McDonald, FUNDAMENTALS OF DIGITAL SWITCHING at 211 (1990) ("The ARPANET was, in part, an experimental verification of the packet switching concept. Robert's objective was a new capability for resource sharing.").

From Two Small Nodes, a Mighty Web Has Grown

By 1966, with these and other basic ideas in place, Lawrence Roberts, recruited by ARPA from the Massachusetts Institute of Technology, mapped out the plan. Two years after the first transmission, the number of host computers grew to 23. The @ symbol was invented in 1972, and a year later 75 percent of the Arpanet traffic was E-mail. It was starting to look like the Net.").

George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES at F1 (October 12, 1999).

20. After leaving ARPANET, Dr. Roberts grew increasingly concerned that existing technologies for routing data packets were incapable of addressing the increasing amounts of data traversing the internet.[12] Dr. Roberts identified that as the "Net grows, the more loss and transmission of data occurs. Eventually, gridlock will set in."[13]

> ***The Internet is broken. I should know*: *I designed it***. In 1967, I wrote the first plan for the ancestor of today's Internet, the Advanced Research Projects Agency Network, or ARPANET, and then led the team that designed and built it. The main idea was to share the available network infrastructure by sending data as small, independent packets, which, though they might arrive at different times, would still generally make it to their destinations. The small computers that directed the data traffic-I called them Interface Message Processors, or IMPs-evolved into today's routers, and for a long time they've kept up with the Net's phenomenal growth. Until now.

Lawrence Roberts, *A Radical New Router*, IEEE SPECTRUM Vol. 46(7) at 34 (August 2009) (emphasis added).

21. In 1998, Dr. Roberts founded Caspian Networks.[14] At Caspian Networks, Dr. Roberts developed a new kind of internet router to efficiently route packets over a network. This

[12] eWeek Editors, *Feeling A Little Congested,* EWEEK MAGAZINE (September 24, 2001) ("Lawrence Roberts, one of the primary developers of Internet precursor ARPANet and CTO of Caspian Networks, recently released research indicating that Net traffic has quadrupled during the past year alone.").

[13] Michael Cooney, *Can ATM Save The Internet,* NETWORK WORLD at 16 (May 20, 1996); Lawrence Roberts, A RADICAL NEW ROUTER, IEEE Spectrum Vol. 46 34-39 (August 2009).

[14] Caspian Networks, Inc. was founded in 1998 as Packetcom, LLC and changed its name to

new router was aimed at addressing concerns about network "gridlock." In a 2001 interview with Wired Magazine, Dr. Roberts discussed the router he was developing at Caspian Networks – the Apeiro. "Roberts says the Apeiro will also create new revenue streams for the carriers by solving the 'voice and video problem.' IP voice and video, unlike email and static Web pages, breaks down dramatically if there's a delay - as little as a few milliseconds - in getting packets from host to recipient."[15]

Jim Duffy, *Router Newcomers take on Cisco, Juniper*, NETWORK WORLD at 14 (April 14, 2013); Stephen Lawson, *Caspian Testing Stellar Core Offering*, NETWORK WORLD at 33 (December 17, 2001); Tim Greene, *Caspian Plans Superfast Routing For The 'Net Core*, NETWORK WORLD at 10 (January 29, 2001); Andrew P. Madden, *Company Spotlight*: *Caspian Networks*, MIT TECHNOLOGY REVIEW at 33 (August 2005); and Loring Wirbel, *Caspian Moves Apeiro Router To Full Availability*, EE TIMES (April 14, 2003).

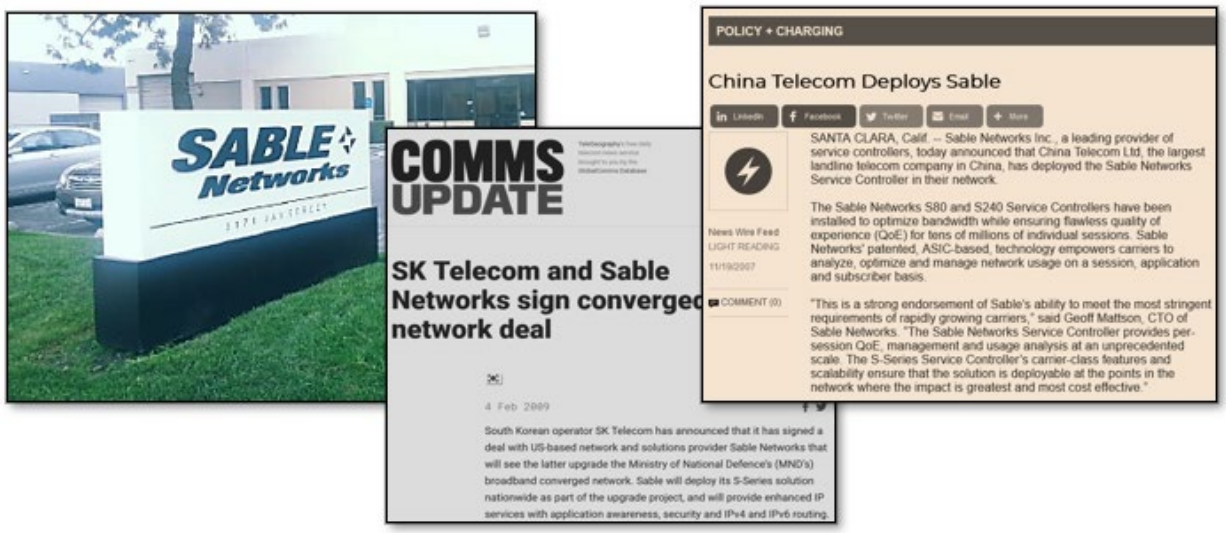
22. The Apeiro debuted in 2003. The Apeiro, a flow-based router, can identify the nature of a packet – be it audio, text, or video, and prioritize it accordingly. The Apeiro included numerous technological advances including quality of service (QoS) routing and flow-based routing.

Caspian Networks, Inc. in 1999.

[15] John McHugh, *The n-Dimensional Superswitch*, WIRED MAGAZINE (May 1, 2001).

23. At its height, Caspian Networks Inc. raised more than $300 million dollars and grew to more than 320 employees in the pursuit of developing and commercializing Dr. Roberts' groundbreaking networking technologies, including building flow-based routers that advanced quality of service and load balancing performance. However, despite early success with its technology and business, Caspian hit hard times when the telecommunications bubble burst.

24. Sable Networks, Inc. was formed by Dr. Sang Hwa Lee to further develop and commercialize the flow-based networking technologies developed by Dr. Roberts and Caspian Networks.[16] Sable Networks, Inc. has continued its product development efforts and has gained commercial success with customers in Japan, South Korea, and China. Customers of Sable Networks, Inc. have included: SK Telecom, NTT Bizlink, Hanaro Telecom, Dacom Corporation, USEN Corporation, Korea Telecom, China Unicom, China Telecom, and China Tietong.

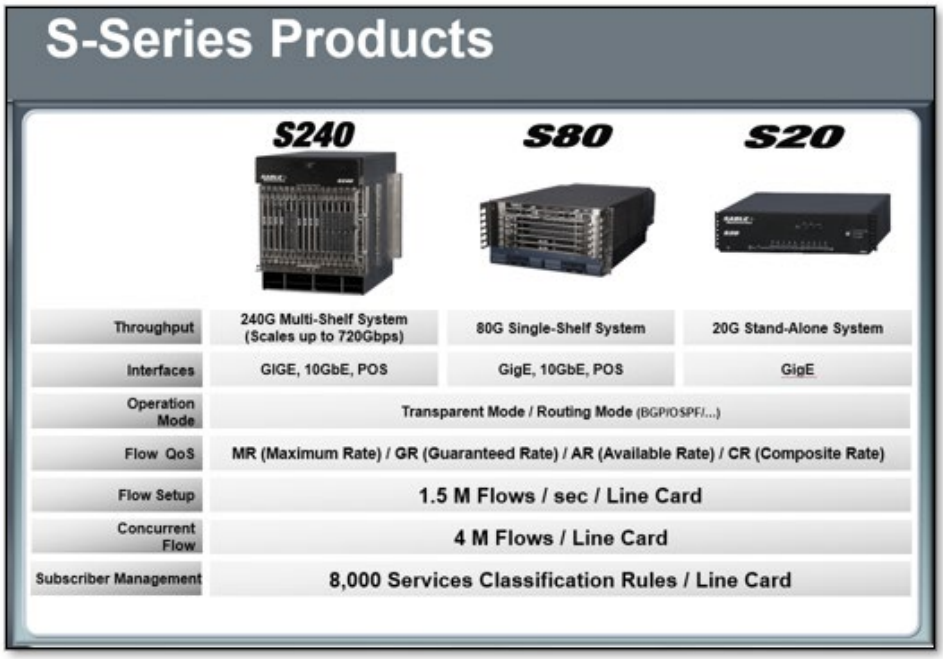


SK Telecom and Sable Networks Sign Convergence Network Deal, COMMS UPDATE – TELECOM NEWS SERVICE (February 4, 2009) ("South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks."); *China Telecom Deploys Sable*, LIGHT READING NEWS FEED (November 19, 2007) ("Sable Networks Inc., a leading provider of service controllers, today announced that China Telecom Ltd, the largest landline

[16] Dr. Lee, through his company Mobile Convergence, Ltd. purchased the assets of Caspian Networks Inc. and subsequently created Sable Networks, Inc.

telecom company in China, has deployed the Sable Networks Service Controller in their network.").

25. Armed with the assets of Caspian Networks, Inc. as well as members of Caspian Networks' technical team, Sable Networks, Inc. continued the product development efforts stemming from Dr. Roberts' flow-based router technologies. Sable Networks, Inc. developed custom application-specific integrated circuits ("ASIC") designed for flow traffic management. Sable Network, Inc.'s ASICs include the Sable Networks SPI, which enables 20 Gigabit flow processing. In addition, Sable Networks, Inc. developed and released S-Series Service Controllers (*e.g.*, S80 and S240 Service Controller models) that contain Sable Networks' flow-based programmable ASICs, POS and Ethernet interfaces, and carrier-hardened routing and scalability from 10 to 800 Gigabits.



SABLE NETWORKS S-SERIES SERVICE CONTROLLERS (showing the S240-240G Multi-Shelf System, S80-80G Single-Shelf System, and S20-20G Stand-Alone System).

26. Sable pursues the reasonable royalties owed for Defendants' use of the inventions claimed in Sable's patent portfolio, which arise from Caspian Networks and Sable Networks' groundbreaking technology.

SABLE'S PATENT PORTFOLIO

27. Sable's patent portfolio includes over 34 patent assets, including 14 granted U.S. patents. Dr. Lawrence Roberts' pioneering work on QoS traffic prioritization, flow-based switching and routing, and the work of Dr. Roberts' colleagues at Caspian Networks Inc. and Sable Networks, Inc. are claimed in the various patents owned by Sable.

28. Highlighting the importance of the patents-in-suit is the fact that the Sable's patent portfolio has been cited by over 1,000 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the computer networking field. Sable's patents have been cited by companies such as:

- Cisco Systems, Inc.[17]
- Juniper Networks, Inc.[18]
- Broadcom Limited[19]
- EMC Corporation[20]
- F5 Networks, Inc.[21]
- Verizon Communications Inc.[22]
- Microsoft Corporation[23]

[17] *See, e.g.*, U.S. Patent Nos. 7,411,965; 7,436,830; 7,539,499; 7,580,351; 7,702,765; 7,817546; 7,936,695; 8,077,721; 8,493,867; 8,868,775; and 9,013,985.

[18] *See, e.g.*, U.S. Patent Nos. 7,463,639; 7,702,810; 7,826,375; 8,593,970; 8,717,889; 8,811,163; 8,811,183; 8,964,556; 9,032,089; 9,065,773; and 9,832,099.

[19] *See, e.g.*, U.S. Patent No. 7,187,687; 7,206,283; 7,266,117; 7,596,139; 7,649,885; 8,014,315; 8,037,399; 8,170,044; 8,194,666; 8,271,859; 8,448,162; 8,493,988; 8,514,716; and 7,657,703.

[20] *See, e.g.*, U.S. Patent Nos. 6,976,134; 7,185,062; 7,404,000; 7,421,509; 7,864,758; and 8,085,794.

[21] *See, e.g.*, U.S. Patent Nos. 7,206,282; 7,580,353; 8,418,233; 8,565,088; 9,225,479; 9,106,606; 9,130,846; 9,210,177; 9,614,772; 9,967,331; and 9,832,069.

[22] *See, e.g.*, U.S. Patent Nos. 7,349,393; 7,821,929; 8,218,569; 8,289,973; 9,282,113; and 8,913,623.

[23] *See, e.g.*, U.S. Patent Nos. 7,567,504; 7,590,736; 7,669,235; 7,778,422; 7,941,309; 7,636,917; 9,571,550; and 9,800,592.

- Intel Corporation[24]
- Extreme Networks, Inc.[25]
- Huawei Technologies Co., Ltd.[26]

THE PARTIES

SABLE NETWORKS, INC.

29. Sable Networks, Inc. ("Sable Networks") is a corporation organized and existing under the laws of the State of California.

30. Sable Networks was formed to continue the research, development, and commercialization work of Caspian Networks Inc., which was founded by Dr. Lawrence Roberts to provide flow-based switching and routing technologies to improve the efficiency and quality of computer networks.

31. Sable Networks is the owner by assignment of all of the patents-in-suit.

SABLE IP, LLC

32. Sable IP, LLC ("Sable IP") is a Delaware limited liability company with its principal place of business at 225 S. 6th Street, Suite 3900, Minneapolis, Minnesota 55402. Pursuant to an exclusive license agreement with Sable Networks, Sable IP is the exclusive licensee of the patents-in-suit.

FORTINET, INC.

33. Fortinet, Inc. ("Fortinet"), is a Delaware corporation with its principal place of business at 1090 Kifer Road, Sunnyvale, California 94086. Fortinet may be served through its

[24] *See, e.g.*, U.S. Patent Nos. 7,177,956; 7,283,464; 9,485,178; 9,047,417; 8,718,096; 8,036,246; 8,493,852; and 8,730,984.

[25] *See, e.g.*, U.S. Patent Nos. 7,903,654; 7,978,614; 8,149839; 10,212,224; 9,112,780; and 8,395,996.

[26] *See, e.g.*, U.S. Patent Nos. 7,903,553; 7,957,421; 10,015,079; 10,505,840; and Chinese Patent Nos. CN108028828 and CN106161333.

registered agent Corporation Service Company dba CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701. Fortinet is registered to do business in the State of Texas and has been since at least November 28, 2000.

34. Fortinet conducts business operations within the Eastern District of Texas where it sells, develops, and/or markets its products including facilities at 6111 W. Plano Parkway, Plano, Texas 75093.

MASERGY COMMUNICATIONS, INC.

35. Masergy Communications, Inc. ("Masergy") is a Delaware corporation with its principal place of business at 2740 Dallas Parkway #260, Plano, Texas 75093. Masergy may be served through its registered agent CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701. Masergy's headquarters and primary place of business is in Plano, Texas, and Masergy has been registered to do business in the State of Texas since September 29, 2000.

JURISDICTION AND VENUE

36. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

37. This Court has personal jurisdiction over Defendants in this action because Defendants have committed acts within the Eastern District of Texas giving rise to this action and have established minimum contacts with this forum such that the exercise of jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice. Defendants, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), have committed and continue to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe one or more of the patents-

in-suit. Moreover, Defendants have registered to do business in the State of Texas, have offices and facilities in the State of Texas, and actively direct their activities to customers located in the State of Texas.

38. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Fortinet is registered to do business in the State of Texas, has offices in the State of Texas, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas. Defendant Masergy is registered to do business in the State of Texas, has its principal office and headquarters in the Eastern District of Texas, and has committed acts of direct and indirect infringement in the Eastern District of Texas.

39. Defendants have regular and established places of business in this District and have committed acts of infringement in this District. Fortinet has a permanent office location at 6111 W. Plano Parkway, Plano, Texas 75093, which is located within this District. Fortinet employs full-time personnel such as sales personnel and engineers in this District, including in Plano, Texas. Fortinet has also committed acts of infringement in this District by commercializing, marketing, selling, distributing, testing, and servicing certain accused products. Masergy is headquartered out of its principal offices, located at 2740 Dallas Parkway #260, Plano, Texas 75093, which is in this District. Masergy has also committed acts of infringement in this District by marketing, selling, distributing, testing, and servicing certain accused products.

40. This Court has personal jurisdiction over Defendants. Defendants have conducted and does conduct business within the State of Texas. Defendants, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including by providing interactive web pages) their products and/or services in the United States and the Eastern District of Texas and/or contribute to and

actively induce customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of an interactive web page) infringing products and/or services in the United States and the Eastern District of Texas. Defendants, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), have purposefully and voluntarily placed one or more infringing products and/or services, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers and/or consumers in the Eastern District of Texas. These infringing products and/or services have been and continue to be made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in the Eastern District of Texas. Defendants have committed acts of patent infringement within the Eastern District of Texas. Defendants interact with customers in Texas, including through visits to customer sites in Texas. Through these interactions and visits, Defendants directly infringe one or more of the patents-in-suit. Defendants also interact with customers who sell the accused products into Texas, knowing that these customers will sell the accused products into Texas, either directly or through intermediaries.

41. Defendants have minimum contacts with this District such that the maintenance of this action within this District would not offend traditional notions of fair play and substantial justice. Thus, the Court therefore has both general and specific personal jurisdiction over Defendants.

42. Joinder of the Defendants is proper under 35 U.S.C. § 299. Common questions of fact relating to Defendants' infringement arise in this action. These common questions include questions concerning Masergy and Fortinet's infringement of the patents-in-suit through the incorporation of common SD-WAN components in the accused Masergy-Fortinet SD-WAN offerings. Common questions of fact as to the profits and revenues derived by Fortinet and

Masergy will arise. Common questions of fact will also exist with regard to Masergy and Fortinet's defenses, if any, in this litigation.

THE ASSERTED PATENTS

U.S. PATENT NO. 6,954,431

43. U.S. Patent No. 6,954,431 (the "'431 patent") entitled, *Micro-Flow Management*, was filed on December 6, 2001, and claims priority to April 19, 2000. The '431 patent is subject to a 35 U.S.C. § 154(b) term extension of 722 days. Sable Networks, Inc. is the owner by assignment of the '431 patent. Sable IP is the exclusive licensee of the '431 patent. A true and correct copy of the '431 patent is attached hereto as Exhibit A.

44. The '431 patent discloses novel methods and systems for managing data traffic comprising a plurality of micro-flows through a network.

45. The inventions disclosed in the '431 patent improve the quality of service in data transmissions over a computer network by relying on per micro-flow state information that enables rate and delay variation requirements to be within set quantified levels of service.

46. The '431 patent discloses technologies that speed the rate at which data can effectively travel over a computer network by optimizing packet discarding.

47. The '431 patent discloses the use of micro-flow state information to determine the rate of each flow, thus optimizing discards and optimizing the quality of service of data transmission.

48. The '431 patent discloses methods and systems that avoid networking system degradation by not overloading network switch buffers.

49. The '431 patent discloses a method for managing data traffic through a network that determines a capacity of a buffer containing a micro-flow based on a characteristic.

50. The '431 patent discloses a method for managing data traffic through a network that assigns an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

51. The '431 patent discloses a method for managing data traffic through a network that delegates a portion of available bandwidth in the network to the micro-flow.

52. The '431 patent discloses a method for managing data traffic through a network that uses the buffer for damping jitter associated with the micro-flow.

53. The '431 patent has been cited by 103 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '431 patent as relevant prior art:

- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Broadcom Limited
- Intel Corporation
- Sun Microsystems, Inc.
- Oracle Corporation
- Samsung Electronics Co., Ltd.
- Adtran, Inc.
- Time Warner Cable, Inc.
- FSA Technologies, Inc.
- Internap Corporation
- France Telecom
- The Boeing Company
- Wistaria Trading, Ltd.

U.S. PATENT NO. 8,243,593

54. U.S. Patent No. 8,243,593 entitled, *Mechanism for Identifying and Penalizing Misbehaving Flows in a Network*, was filed on December 22, 2004. The '593 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,098 days. Sable Networks, Inc. is the owner by assignment of the '593 patent. Sable IP is the exclusive licensee of the '593 patent. A true and correct copy of the '593 patent is attached hereto as Exhibit B.

55. The '593 patent discloses novel methods and systems for processing a flow of a series of information packets.

56. The inventions disclosed in the '593 patent teach technologies that permit the identification and control of less desirable network traffic.

57. Because the characteristics of data packets in undesirable network traffic can be disguised, the '593 patent improves the operation of computer networks by disclosing technologies that monitor the characteristics of flows of data packets rather than ancillary factors such as port numbers or signatures.

58. The '593 patent discloses tracking the behavioral statistics of a flow of data packets that can be used to determine whether the flow is undesirable.

59. The '593 patent further discloses taking actions to penalize the flow of undesirable network traffic.

60. The '593 patent discloses a method for processing a flow of a series of information packets that maintains a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

61. The '593 patent discloses a method for processing a flow of a series of information packets that determines, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

62. The '593 patent discloses that the determination as to whether the flow is exhibiting undesirable behavior is made regardless of the presence or absence of congestion.

63. The '593 patent discloses a method for processing a flow of data packets that enforces a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

64. The '593 patent has been cited by 17 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '593 patent as relevant prior art.

- Cisco Systems, Inc.
- AT&T, Inc.
- International Business Machines Corporation
- Telecom Italia S.p.A.
- McAfee, LLC

U.S. PATENT NO. 8,817,790

65. U.S. Patent No. 8,817,790 (the "'790 patent") entitled, *Identifying Flows Based on Behavior Characteristics and Applying User-Defined Actions*, was filed on September 23, 2011, and claims priority to July 31, 2006. Sable Networks, Inc. is the owner by assignment of the '790 patent. Sable IP is the exclusive licensee of the '790 patent. A true and correct copy of the '790 patent is attached hereto as Exhibit C.

66. The '790 patent claims specific methods and devices for handling a flow of information packets.

67. The '790 patent discloses methods and systems for efficiently identifying undesirable traffic over data networks.

68. The '790 patent teaches technologies that identify traffic not by inspecting the payload of each data packet, but rather by analyzing and classifying the behavior of the data flows to identify undesirable traffic.

69. The '790 patent discloses applying a user-specified action associated with a policy applicable to data flows that are designated undesirable.

70. The '790 patent discloses a method of handling a flow that processes a flow comprised of two or more information packets having header information in common.

71. The '790 patent discloses a method of handling a flow that stores header-independent statistics about the flow in a flow block associated with the flow.

72. The '790 patent discloses a method of handling a flow that updates the header-independent statistics in the flow block as each information packet belonging to the flow is processed.

73. The '790 patent discloses a method of handling a flow that categorizes the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type.

74. The '790 patent discloses a method of handling a flow that performs an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

75. The '790 patent family has been cited by 24 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '790 patent family as relevant prior art:

- Cisco Systems, Inc.
- Solana Networks, Inc.
- British Telecommunications Public Limited Company
- Level 3 Communications, LLC
- Calix, Inc.
- Nokia Corporation
- Verizon Communications, Inc.
- Sprint Spectrum L.P.

- Hon Hai Precision Industry Co., Ltd.

U.S. PATENT NO. 9,774,501

76. U.S. Patent No. 9,774,501 (the "'501 patent") entitled, *System and Method for Ensuring Subscriber Fairness Using Outlier Detection*, was filed on September 7, 2016, and claims priority to May 14, 2012. Sable Networks, Inc. is the owner by assignment of the '501 patent. Sable IP is the exclusive licensee of the '501 patent. A true and correct copy of the '501 patent is attached hereto as Exhibit D.

The '501 patent claims specific methods and devices for a subscriber fairness solution that uses flow-based statistical collection mechanism to monitor subscriber usage across various attributes.

77. The '501 patent discloses methods and systems for detecting outlier users of a network resource.

78. The '501 patent teaches technologies for detecting outlier users of a network resource using a fairness model that accounts for the cost of a user's behavior on other users and provides for evaluating and effecting service fairness.

79. The '501 patent discloses aggregating flow data of a user of a network resource for set time periods. The flow data that is aggregated can include connections between a particular source IP address and transport layer port to a particular destination IP address and transport layer port.

80. The '501 patent discloses applying outlier detection logic to the flow-count pattern that is generated for a user and comparing it to flow-count patterns associated with other users on the network.

81. The '501 patent discloses a method of assigning a flow-count band to the user based on the outlier detection logic where the user's flow count is compared to the flow-count data of other users on the network.

82. The '501 patent discloses a method of applying a mitigating action to the user based on the user's access to the network resource based on the flow-count band that the user's activity causes the user to be assigned to.

83. The '510 patent discloses a method of implementing outlier detection for a user on a network using a detection phase and a mitigation phase. In the detection phase, "outliers" are identified - users that are using a disproportionate amount of network resources. In the mitigation phase, actions are taken to restrict the access of the outlier user to network resources.

84. The '501 patent discloses a computer implemented method that improves the function of a computer network through using outlier detection to mitigate an individual user's over use of the network bandwidth.

85. The '501 patent family has been cited by 11 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '501 patent family as relevant prior art:

- Cisco Systems, Inc.
- International Business Machines Corporation
- Google, Inc.
- Adobe, Inc.
- British Telecomm
- VMware, Inc.
- Sprint Spectrum L.P.
- Infinera Corporation

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,954,431

86. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

87. Masergy designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing data traffic comprising a plurality of micro-flows through a network.

88. Masergy designs, makes, sells, offers to sell, imports, and/or uses the Masergy SD-WAN Solution offerings including at least the following product offerings: Masergy SD-WAN Secure,[27] Masergy Co-Managed SD-WAN,[28] Managed SD-WAN Secure OTT,[29] Masergy SD-WAN Home,[30] Masergy SD-WAN Branch solutions,[31] Masergy Secure Access Service Edge

[27] *Answering Partner FAQs On Managed SD-WAN,* MASERGY DOCUMENTATION (2020) ("Masergy SD-WAN Secure solutions are powered by Fortinet to provide customers with integrated security features such as a next-generation firewall").

[28] *Masergy Expands Its SD-WAN Portfolio Offering the Broadest Choice, Flexibility and Built-In SASE,* MASERGY PRESS RELEASE (July 21, 2020) ("Co-managed solutions: Leveraging the SD-WAN Orchestrator, clients can customize their configurations and make changes while Masergy simultaneously monitors and reports on performance.").

[29] *Masergy Managed SD-WAN Secure OTT*: *Internet Strategies Built For Security and Choice,* MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/managed-sd-wan-secure-ott ("How Masergy's SD-WAN Secure OTT works: Masergy creates an overlay network on top of any public or private network and sends encrypted application traffic via IPsec tunnels to Fortinet-powered endpoints over the public internet ('over the top') for your secure, agile, and scalable corporate network.").

[30] Andy Patrizio, *Masergy teams with Fortinet for at-home SD-WAN*, NETWORKWORLD.COM ARTICLE (October 19, 2020) *available at*: https://www.networkworld.com/article/3586177/masergy-teams-with-fortinet-for-at-home-sd-wan.html ("The SD-WAN Secure Home offering utilizes a lightweight Fortinet Secure SD-WAN device for connectivity and improved application performance over a home Internet connection. It also includes built-in next-generation firewall and routing, direct connections to an ecosystem of cloud services").

[31] *Extending secure SD-WAN to secure SD-Branch*: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge ("Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.").

solutions (SASE),[32] and Masergy Secure Web Gateway solutions[33] (collectively, the "Masergy-Fortinet '431 Products").

89. The Masergy-Fortinet '431 Products incorporate Fortinet components running Fortinet OS Version 5.4 and later including Fortinet's FortiGate Next-Generation Firewalls.

> Details of the Masergy SASE offering are as follows: Cloud firewalls in all global points of presence (POPs) powered by Fortinet: Masergy has a number of global POPs where it will offer cloud resident firewalls using Fortinet's FortiGate next-generation firewall (NGFW). Cloud firewalls are fast and easy to deploy and provide corporate-class threat protection to sites that are as small as a single person. It's important to note that Masergy will continue to offer its edge-based service for users that prefer an on-premises appliance. This hybrid approach provides customers with threat protection where they want it, without the associated complexity of managing a highly distributed environment.

Zeus Kerravala, *How Masergy Uses Partners to Provide Secure-Access Service Edge*, EWEEK.COM ARTICLE (November 16, 2020), *available at*: https://www.eweek.com/security/how-masergy-uses-partners-for-secure-access-service-edge (emphasis added).

90. The Masergy-Fortinet '431 Products include Fortinet application-specific integrated circuits ("ASIC"). The Fortinet ASIC chips are purpose build by Fortinet for SD-WAN solutions such as the Masergy-Fortinet '431 Products. The following excerpt from a Masergy article describes the incorporation of the Fortinet ASIC in the Masergy-Fortinet '431 Products.

> Best-of-Breed SD-WAN & Security: Fortinet is committed to driving a consistent security posture from the WAN edge to both data centers and multi-cloud environments by natively integrating security functions, including NGFW, IPS, anti-virus, anti-malware, web filtering, SSL inspection (including TLS 1.3), and sandboxing. Fortinet also provides an integrated CASB service to protect SaaS applications and traffic and to prevent problems related to Shadow IT. Our patented innovation of a purpose-built SD-WAN ASIC enables faster Application Steering,

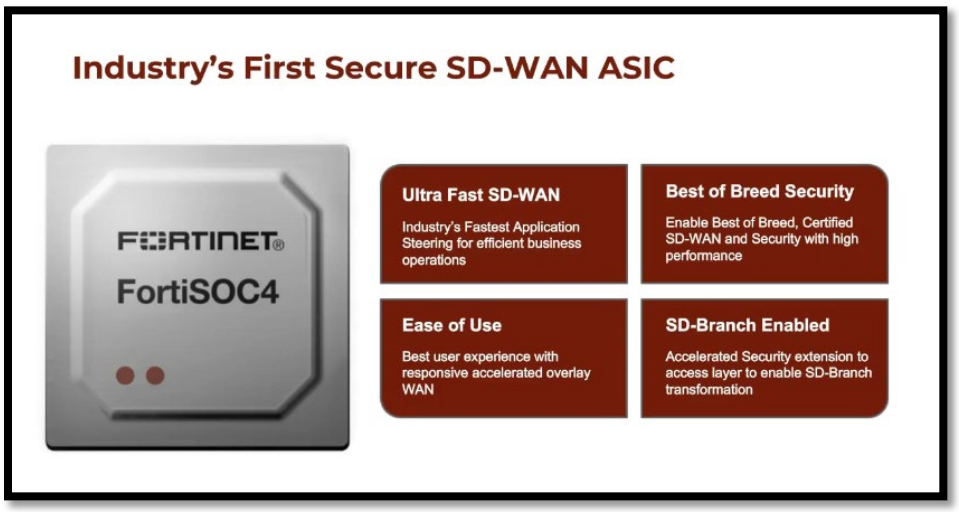
[32] *SASE from Fortinet & Masergy*: *Converging best-of-breed network and security solutions recognized by Gartner,* MASERGY BLOG POSTING (October 6, 2020), *available at*: https://www.masergy.com/blog/sase-from-fortinet-masergy-converging-best-of-breed-network-and-security-solutions-recognized-by-gartner ("Investors seeking out SASE solutions are demanding best-of-breed technologies converged into one solution, and it's here where the Masergy-Fortinet offering stands above the rest.").

[33] *Masergy Secure Web Gateway*, MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/sase/secure-web-gateway ("Masergy's secure web gateway solution is powered by Fortinet . . . Fortinet SWGs go beyond standard web proxies to keep enterprise networks safe from malicious internet traffic, preventing threats from entering the network and causing an infection or intrusion.").

> Multi-Path Intelligence, and WAN Path Remediation with forward error correction (FEC) to overcome adverse WAN conditions.

Fortinet & Masergy: *The security-driven approach to SD-WAN*, MASERGY BLOG POSTING (January 16, 2020), *available at*: https://www.masergy.com/blog/fortinet-masergy-the-security-driven-approach-to-sd-wan (emphasis added).

91. A recent joint Masergy-Fortinet webcast identified that the Masergy-Fortinet '431 Products include a secure SD-WAN ASIC developed by Fortinet. The following excerpt from the webcast shows the functionality of the FortiSOC4 ASIC that is included in the Masergy-Fortinet '431 Products.



Enabling Enterprises with Secure, Agile and Intelligent Managed SD-WAN, Masergy-FORTINET PARTNER WEBCAST (April 29, 2020), *available at*: https://www.fortinet.com/resources-campaign/network.

92. The Masergy-Fortinet '431 Products include Fortinet's SD-WAN devices. Specifically, a February 2020 press release from Fortinet quoted Masergy's Executive Vice President Bob Laskey describing the Masergy-Fortinet '431 Products as built on "Fortinet's Secure SD-WAN" components.

> Built on Fortinet's Secure SD-WAN, Masergy's Managed SD-WAN solution gives clients software-defined network services and three tiered options for managed security services. It's a winning combination that resonates with global enterprises needing cloud application performance, 24/7 threat monitoring, as well as incident response. Like Fortinet, we believe networking and security need to be inextricably tied, and resellers with a Fortinet-Masergy partnership address more needs across both IT domains.

Fortinet Drives Channel Business Opportunities with Secure SD-WAN, FORTINET PRESS RELEASE (February 5, 2020) (quote from Bob Laskey, Masergy Executive Vice President).

93. The Masergy-Fortinet '431 Products include Fortinet's FortiGate devices that contain functionality for SD-WAN, routing, and next-generation firewall protection. The integration of Fortinet's FortiGate devices into the Masergy-Fortinet '431 Products enables the Masergy-Fortinet '431 Products to infringe the '431 patent claims. The following excerpt from documentation of the Masergy-Fortinet '431 Products states that Masergy delivers secure SD-WAN solutions using a Fortinet FortiGate hardware endpoint.

Managed SD-WAN by Masergy

As a 20-year pioneer in software-defined networking, Masergy is a leading managed services provider delivering SD-WAN, unified communications, and managed security solutions to global enterprises.

Masergy delivers secure SD-WAN solutions to customers using a customized Fortinet FortiGate hardware endpoint. The customized FortiGate device is pre-provisioned with features including SD-WAN, routing, next-generation firewall (with options for additional unified threat management protection, 24/7 threat monitoring and incident response, and more); and enables the addition of secure LAN switching and secure Wi-Fi, all with centralized policy management.

While Masergy can ship out a small appliance for critical or power remote users to extend full functionality of SD-WAN features, remote users can also connect to Masergy's global network and cloud platform via VPNs. Businesses can seamlessly deploy remote VPN connections due to the software-defined networking (SDN) elements built into Masergy's network. The SDN-enabled platform ensures fast and easy deployment and disconnection of connections, tunnels, links, loops, and bandwidth, compared to legacy networks governed by manual processes.

Roopa Honnachari, *COVID-19 Highlights the Business Case for Extending SD-WAN to Remote Workers,* BUSINESS COMMUNICATION SERVICES (BCS) VOL. 14 NO. 1 at 8 (May 2020) (emphasis added).

94. The Masergy-Fortinet '431 Products incorporate Fortinet's FortiGate Next Generation Firewall and SD-WAN components. A November 2020 article describing the Masergy-Fortinet '431 Products stated that Masergy combined Fortinet's FortiGate Next Generation Firewall and SD-WAN components into a "single platform."

> Masergy has bulked up its own SD-WAN Secure solution to make a bigger play into the SASE space by expanding cloud firewalls into all of its global points-of-presence (POPs). Masergy announced on Monday that it had integrated Fortinet's FortiGate Next-Generation Firewalls integrate NGFW and SD-WAN capabilities

> onto a single platform and deployed them in all of its software-defined network POPs as well as integrated them into its SD-WAN and security policies.

Mike Robuck, *Masergy goes bigger and bolder into SASE arena by taking best-of-breed approach,* FIERCETELECOM.COM ARTICLE (November 16, 2020), *available at*: https://www.fiercetelecom.com/telecom/masergy-goes-bigger-and-bolder-into-sase-arena (emphasis added).

95. The Masergy-Fortinet '431 Products include Fortinet's Secure SD-WAN with "built-in Next-Generation Firewall (NGFW) capabilities . . . Fortinet Secure SD-WAN is powered by [a] purpose-built SD-WAN processor." The following excerpt from an April 2020 article authored by Masergy describes the inclusion of the Fortinet SD-WAN components in the Masergy-Fortinet '431 Products.

The security-driven approach to SD-Branch: Fortinet and Masergy

Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.

SD-WAN with built-in security including next-gen firewalls and advanced routing

- Fortinet Secure SD-WAN with built-in Next-Generation Firewall (NGFW) capabilities offers robust security, connectivity, and management across the branch environment. Fortinet Secure SD-WAN is powered by purpose-built SD-WAN processor, combined with advanced network traffic management functionality such as application steering to ensure high application performance on any WAN link. Fortinet Secure SD-WAN has been recommended twice by NSS Labs consecutively in SD-WAN group tests and trusted by over 21,000 customers.

Extending secure SD-WAN to secure SD-Branch: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge

96. One or more of the Masergy-Fortinet '431 Products include technology for managing data traffic comprising a plurality of micro-flows through a network.

97. One or more of the Masergy-Fortinet '431 Products determine the capacity of a buffer containing a micro-flow based on a characteristic.

98. One or more of the Masergy-Fortinet '431 Products assign an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

99. One or more of the Masergy-Fortinet '431 Products delegate a portion of available bandwidth in the network to the micro-flow.

100. The Masergy-Fortinet '431 Products enable the setting of thresholds for a buffer that include the ability to set a threshold as a percentage of the buffer.

101. One or more of the Masergy-Fortinet '431 Products use the buffer for damping jitter associated with the micro-flow.

102. The Masergy-Fortinet '431 Products use buffers to limit jitter which is delay variance.

103. Masergy has directly infringed and continues to directly infringe the '431 patent by, among other things, making, using, offering for sale, and/or selling technology for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Masergy-Fortinet '431 Products.

104. The Masergy-Fortinet '431 Products are available to businesses and individuals throughout the United States.

105. The Masergy-Fortinet '431 Products are provided to businesses and individuals located in the Eastern District of Texas.

106. By making, using, testing, offering for sale, and/or selling products and services for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Masergy-Fortinet '431 Products, Masergy has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '431 patent, including at least claims 10-16, 19, and 24-32 pursuant to 35 U.S.C. § 271(a).

107. Fortinet indirectly infringes the '431 patent by actively inducing infringement under 35 U.S.C. § 271(b).

108. Fortinet has had knowledge of the '431 patent since at least service of this Complaint or shortly thereafter, and Fortinet knew of the '431 patent and knew of its infringement, including by way of this lawsuit.

109. Alternatively, Fortinet has had knowledge of the '431 patent since at least November 9, 2020, or shortly thereafter. On November 9, 2020, Sable Networks, Inc. and Sable IP, LLC produced the Sable Networks-Sable IP Patent Exclusive License Agreement at SBL-VNU_0000001-SBL-VNU_0000008 in the *Sable Networks, Inc., et al. v. Fortinet, Inc.*, No. 5:20-cv-00109-RWS (E.D. Tex.) action currently pending in this district. The Sable Networks-Sable IP Patent Exclusive License Agreement identifies the '431 patent and was produced to Fortinet.

110. Alternatively, Fortinet has had knowledge of the '431 patent since at least June 17, 2020, or shortly thereafter. Fortinet is a Defendant in a related patent infringement action asserted by the Plaintiffs in this action that is currently pending in this District, *Sable Networks, Inc., et al. v. Fortinet, Inc.*, No. 5:20-cv-00109-RWS (E.D. Tex.). Plaintiffs are presently asserting the '431 patent against competitors of Fortinet in three co-pending cases in the Western District of Texas: *Sable Networks, Inc., et al. v. Cisco Sys., Inc.*, No. 6:20-cv-00288-ADA (W.D. Tex.); *Sable Networks, Inc., et al. v. Juniper Networks, Inc.*, No. 6:20-cv-00524-ADA (W.D. Tex.); and *Sable Networks, Inc., et al. v. Nokia Corp., et al.*, No. 6:20-cv-00808-ADA (W.D. Tex.). The *Cisco* and *Juniper* co-pending cases in the Western District of Texas were both on file prior to the date Fortinet was served with the Complaint in *Sable Networks, Inc., et al. v. Fortinet, Inc.*, No. 5:20-cv-00109-RWS (E.D. Tex.), which was June 17, 2020. On information and belief, Fortinet has had knowledge of the '431 patent since at least June 17, 2020, or shortly thereafter.

111. Alternatively, Fortinet has had knowledge of the '431 patent since at least February 7, 2018. On February 7, 2018, Fortinet filed a petition for *Inter Partes* Review of U.S. Patent No. 8,111,629 before the U.S. Patent and Trademark Office's Patent Trial and Appeal Board. *See* IPR2018-00594, Paper 1 (PTAB Feb. 7, 2018). U.S. Patent No. 8,085,775 (the "'775 patent"), which is owned by Sable Networks, Inc. was the primary prior art reference analyzed by Fortinet in this *Inter Partes* Review petition. *See* Paper 1 at 26 (identifying the '775 patent either alone or in combination with another reference as "Ground 1" for its argument that the claims of U.S. Patent No. 8,111,629 were invalid). Fortinet then described and analyzed the '775 patent for the next 10 pages of the *Inter Partes* Review petition. *See* Paper 1 at 26-36. On information and belief, Fortinet studied the Sable patent portfolio, which includes the '775 patent in addition to each of the patents-in-suit in this action, in connection with its research and preparation of its *Inter Partes* Review petition seeking the invalidation of U.S. Patent No. 8,111,629. Based upon the extensive analysis of the '775 patent contained in the *Inter Partes* Review petition, on information and belief, Fortinet reviewed each of the patents-in-suit in this case, including the '431 patent, before selecting the '775 patent as Fortinet's primary prior art reference to argue the invalidity of U.S. Patent No. 8,111,629.

112. Fortinet intended to induce patent infringement by third-party customers and users of the Masergy-Fortinet '431 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Fortinet specifically intended and was aware that the normal and customary use of the accused products would infringe the '431 patent. Fortinet performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '431 patent and with the knowledge that the induced acts would constitute infringement. For example, Fortinet

provides the Masergy-Fortinet '431 Products that have the capability of operating in a manner that infringe one or more of the claims of the '431 patent, including at least claims 10-16, 19, and 24-32, and Fortinet further provides documentation and training materials that cause customers and end users of the Masergy-Fortinet '431 Products to utilize the products in a manner that directly infringe one or more claims of the '431 patent.[34] By providing instruction and training to customers and end-users on how to use the Masergy-Fortinet '431 Products in a manner that directly infringes one or more claims of the '431 patent, including at least claims 10-16, 19, and 24-32, Fortinet specifically intended to induce infringement of the '431 patent. Fortinet engaged in such inducement to promote the sales of the Masergy-Fortinet '431 Products, e.g., through Fortinet user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '431 patent. Accordingly, Fortinet has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '431 patent, knowing that such use constitutes infringement of the '431 patent.

113. Fortinet also indirectly infringes the '431 patent by contributing to the infringement of the '431 patent under 35 U.S.C. § 271(c).

[34] *See e.g., Fortinet Drives Channel Business Opportunities with Secure SD-WAN*, FORTINET PRESS RELEASE (February 5, 2020); *Fortinet Customer Profile*: *Masergy - Partnering with Fortinet to Deliver a Security-Driven Approach to SD-WAN and SD-Branch*, FORTINET.COM WEBSITE (last visited December 2020), *available at*: https://www.fortinet.com/customers/masergy; *Enabling Enterprises with Secure, Agile and Intelligent Managed SD-WAN*, MASERGY-FORTINET PARTNER WEBCAST (April 29, 2020), *available at*: https://www.fortinet.com/resources-campaign/network; *Driving Growth, Security, and Business Efficiency with Managed SD-WAN Services*, FORTINET PARTNER WEBCAST (September 16, 2020), *available at*: https://events.fortinet.com/WeeklyWebinarSeries/session/32051 (joint webcast hosted by Fortinet featuring speakers from Masergy and Fortinet); FORTICLIENT - ADMINISTRATION GUIDE VERSION 6.4.1 (August 24, 2020); *Fortinet Secure SD-WAN Reference Architecture,* FORTINET WHITE PAPER (April 3, 2019); FORTIOS HANDBOOK - PARALLEL PATH PROCESSING (LIFE OF A PACKET) VERSION 5.6.7 (March 15, 2019); and FORTIOS – COOKBOOK VERSION 6.2.4 (June 1, 2020).

114. Fortinet contributes to the infringement of one or more claims of the '431 patent by offering to sell, selling, and/or importing into the United States one or more components of the Masergy-Fortinet '431 Products that constitutes a material part of the invention, knowing that said components are especially made or especially adapted for use in infringing the '431 patent, including at least claims 10-16, 19, and 24-32, and are not staple articles or commodities of commerce suitable for substantial non-infringing use. The Masergy-Fortinet '431 Products are contain Fortinet OS version 5.4 and later, which are programmed with specific software components, *e.g.* Fortinet SD-WAN Traffic Shaping and QoS. These software components, which are incorporated into and sold as part of the Masergy-Fortinet '431 Products, are supplied by Fortinet and are especially made for use in systems that infringe the '431 patent, including at least claims 10-16, 19, and 24-32, and have no substantial non-infringing uses.

115. The '431 patent is well-known within the industry as demonstrated by multiple citations to the '431 patent in published patents and patent applications assigned to technology companies and academic institutions. Defendants are utilizing the technology claimed in the '431 patent without paying a reasonable royalty. Defendants are infringing the '431 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

116. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '431 patent.

117. As a result of Defendants' infringement of the '431 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 8,243,593

118. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

119. Masergy designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for processing a flow of a series of information packets.

120. Masergy designs, makes, sells, offers to sell, imports, and/or uses devices that enable the identification and penalization of data flows based on the behavior of the data flow, including at least the Masergy SD-WAN Solution offerings including the following products: Masergy SD-WAN Secure,[35] Masergy Co-Managed SD-WAN,[36] Managed SD-WAN Secure OTT,[37] Masergy SD-WAN Home,[38] Masergy SD-WAN Branch solutions,[39] Masergy Secure

[35] *Answering Partner FAQs On Managed SD-WAN,* MASERGY DOCUMENTATION (2020) ("Masergy SD-WAN Secure solutions are powered by Fortinet to provide customers with integrated security features such as a next-generation firewall").

[36] *Masergy Expands Its SD-WAN Portfolio Offering the Broadest Choice, Flexibility and Built-In SASE,* MASERGY PRESS RELEASE (July 21, 2020) ("Co-managed solutions: Leveraging the SD-WAN Orchestrator, clients can customize their configurations and make changes while Masergy simultaneously monitors and reports on performance.").

[37] *Masergy Managed SD-WAN Secure OTT*: *Internet Strategies Built For Security and Choice,* MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/managed-sd-wan-secure-ott ("How Masergy's SD-WAN Secure OTT works: Masergy creates an overlay network on top of any public or private network and sends encrypted application traffic via IPsec tunnels to Fortinet-powered endpoints over the public internet ('over the top') for your secure, agile, and scalable corporate network.").

[38] Andy Patrizio, *Masergy teams with Fortinet for at-home SD-WAN*, NETWORKWORLD.COM ARTICLE (October 19, 2020) *available at*: https://www.networkworld.com/article/3586177/masergy-teams-with-fortinet-for-at-home-sd-wan.html ("The SD-WAN Secure Home offering utilizes a lightweight Fortinet Secure SD-WAN device for connectivity and improved application performance over a home Internet connection. It also includes built-in next-generation firewall and routing, direct connections to an ecosystem of cloud services").

[39] *Extending secure SD-WAN to secure SD-Branch*: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge ("Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.").

Access Service Edge solutions (SASE),[40] and Masergy Secure Web Gateway solutions[41] (collectively, the "Masergy-Fortinet '593 Products").

121. The Masergy-Fortinet '593 Products incorporate Fortinet's FortiGate Next-Generation Firewalls with Fortinet OS version 6.2 and later.

> Details of the Masergy SASE offering are as follows: Cloud firewalls in all global points of presence (POPs) powered by Fortinet: Masergy has a number of global POPs where it will offer cloud resident firewalls using Fortinet's FortiGate next-generation firewall (NGFW). Cloud firewalls are fast and easy to deploy and provide corporate-class threat protection to sites that are as small as a single person. It's important to note that Masergy will continue to offer its edge-based service for users that prefer an on-premises appliance. This hybrid approach provides customers with threat protection where they want it, without the associated complexity of managing a highly distributed environment.

Zeus Kerravala, *How Masergy Uses Partners to Provide Secure-Access Service Edge*, EWEEK.COM ARTICLE (November 16, 2020), *available at*: https://www.eweek.com/security/how-masergy-uses-partners-for-secure-access-service-edge (emphasis added).

122. The Masergy-Fortinet '593 Products include Fortinet's Application-Specific Integrated Circuits (ASIC). The Fortinet ASIC included in the Masergy-Fortinet '593 Products process data packets associated with a data flow. The ASIC chips are purpose-built by Fortinet for SD-WAN solutions. The following excerpt from a Masergy article describes the incorporation of the Fortinet ASIC in the Masergy-Fortinet '593 Products.

> Best-of-Breed SD-WAN & Security: Fortinet is committed to driving a consistent security posture from the WAN edge to both data centers and multi-cloud environments by natively integrating security functions, including NGFW, IPS, anti-virus, anti-malware, web filtering, SSL inspection (including TLS 1.3), and sandboxing. Fortinet also provides an integrated CASB service to protect SaaS applications and traffic and to prevent problems related to Shadow IT. Our patented

[40] *SASE from Fortinet & Masergy*: *Converging best-of-breed network and security solutions recognized by Gartner,* MASERGY BLOG POSTING (October 6, 2020), *available at*: https://www.masergy.com/blog/sase-from-fortinet-masergy-converging-best-of-breed-network-and-security-solutions-recognized-by-gartner ("Investors seeking out SASE solutions are demanding best-of-breed technologies converged into one solution, and it's here where the Masergy-Fortinet offering stands above the rest.").

[41] *Masergy Secure Web Gateway*, MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/sase/secure-web-gateway ("Masergy's secure web gateway solution is powered by Fortinet . . . Fortinet SWGs go beyond standard web proxies to keep enterprise networks safe from malicious internet traffic, preventing threats from entering the network and causing an infection or intrusion.").

> innovation of a purpose-built SD-WAN ASIC enables faster Application Steering, Multi-Path Intelligence, and WAN Path Remediation with forward error correction (FEC) to overcome adverse WAN conditions.

Fortinet & Masergy: *The security-driven approach to SD-WAN*, MASERGY BLOG POSTING (January 16, 2020), *available at*: https://www.masergy.com/blog/fortinet-masergy-the-security-driven-approach-to-sd-wan (emphasis added).

123. The following excerpt from a webcast shows the functionality of the SD-WAN components included in the Masergy-Fortinet '593 Products including "Application identification" and "Forward Error Correction."

Enabling Enterprises with Secure, Agile and Intelligent Managed SD-WAN, Masergy-FORTINET PARTNER WEBCAST (April 29, 2020), *available at*: https://www.fortinet.com/resources-campaign/network (annotation added).

124. The Masergy-Fortinet '593 Products include Fortinet's SD-WAN devices that contain a means for maintaining a set of behavioral statistics for the flow. The behavioral statistics are updated based on each information packet belonging to the flow being processed (without consideration for the congestion of the network). Specifically, the Fortinet '593 Products process the data packet upon receipt, and if the data packet does not match an existing flow, a new flow block is created in the flow table. A flow block is a flow entry that is used to match and process packets. Stateful inspection as implemented by the Fortinet '593 Products looks at the first packet of a session and looks in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a

session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed. When the first packet of a session is matched in the policy table, stateful inspection adds information about the session to its session table. When subsequent packets are received for the same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table). Fortinet documentation describes the treatment of packets that share common header information "source/destination IP," "source/destination port," and "protocol" as being part of a flow and being processed in the same manner.

125. A February 2020 press release from Fortinet quoted Masergy's Executive Vice President, Bob Laskey, as describing the Masergy-Fortinet '593 Products as built on "Fortinet's Secure SD-WAN" components. "Built on Fortinet's Secure SD-WAN, Masergy's Managed SD-WAN solution gives clients software-defined network services and three tiered options for managed security services. It's a winning combination that resonates with global enterprises needing cloud application performance, 24/7 threat monitoring, as well as incident response." *Fortinet Drives Channel Business Opportunities with Secure SD-WAN*, FORTINET PRESS RELEASE (February 5, 2020) (quote from Bob Laskey, Masergy Executive Vice President).

126. The Masergy-Fortinet '593 Products include a misbehaving flow manager (MFM) for processing a flow of information packets passed over a network. The Masergy-Fortinet '593 Products include FortiGate devices that contain functionality for SD-WAN, routing, and next-generation firewall protection. The integration of Fortinet's FortiGate devices into the Masergy-Fortinet '593 Products enables the products to infringe the '593 patent claims. The following

excerpt from documentation of the Masergy-Fortinet '593 Products states that Masergy delivers secure SD-WAN solutions using a Fortinet FortiGate hardware endpoint.

> You'll get the broadest SD-WAN options, SASE-based security at the core, controls to reconfigure services on the fly, and unprecedented Service Level Agreements (SLAs) delivering performance perfection. With the only pure software-defined edge network, Masergy is your partner for reliability and business continuity. Fortinet® edge devices and built-in firewalls on premise or in the cloud along with a menu of managed security services offer a holistic approach for the best end-to-end management— enabling employees to work from anywhere.

Masergy SD-WAN Secure, MASERGY SOLUTIONS BRIEF at 1 (2020) (emphasis added).

127. The Masergy-Fortinet '593 Products incorporate Fortinet's FortiGate Next Generation Firewall and SD-WAN products. A November 2020 article describing the Masergy-Fortinet '593 Products stated that Masergy combined Fortinet's FortiGate Next Generation Firewall and SD-WAN components into a "single platform."

> Masergy has bulked up its own SD-WAN Secure solution to make a bigger play into the SASE space by expanding cloud firewalls into all of its global points-of-presence (POPs). Masergy announced on Monday that it had integrated Fortinet's FortiGate Next-Generation Firewalls integrate NGFW and SD-WAN capabilities onto a single platform and deployed them in all of its software-defined network POPs as well as integrated them into its SD-WAN and security policies.

Mike Robuck, *Masergy goes bigger and bolder into SASE arena by taking best-of-breed approach,* FIERCETELECOM.COM ARTICLE (November 16, 2020), *available at*: https://www.fiercetelecom.com/telecom/masergy-goes-bigger-and-bolder-into-sase-arena (emphasis added).

128. The Masergy-Fortinet '593 Products comprise a means for computing if a flow is exhibiting undesirable behavior using at least partially the flow's behavioral statistics which generate a badness factor for the flow. This badness factor indicates if the flow is exhibiting undesirable behavior. The specification of the '593 patent describes that identification of misbehaving flows can be done by done heuristically. Specifically, behavioral statistics about the

flow might not be directly identified with a flow misbehaving but might be strongly indicative of a flow having undesirable characteristics. Using behavioral statistical data as a proxy for making a determination about the quality of a flow is a heuristic technique because it uses data that produces an approximate determination. Specifically, the Fortinet '593 Products use the behavioral statistics (transmission rate, byte count, etc.) to make an approximate determination that a flow is undesirable and could be part of a distributed denial-of-service ("DDoS") attack. Similarly, the '593 patent describes how one can use behavioral statistics to make a determination that a flow is associated with peer-to-peer traffic. The Fortinet '593 Products' use of flow behavior to identify flows that could be part of a DDoS attack is heuristic as they use data about the flow to make an efficient conclusion about the flow.

129. One or more of the Masergy-Fortinet '593 Products include technology for processing a flow of a series of information packets. Specifically, the Masergy-Fortinet '593 Products maintain a set of behavioral statistics based on each and every information packet belonging to a flow.

130. The Masergy-Fortinet '593 Products are available to businesses and individuals throughout the United States.

131. The Masergy-Fortinet '593 Products are provided to businesses and individuals located in the Eastern District of Texas.

132. The Masergy-Fortinet '593 Products include Fortinet's Secure SD-WAN with "built-in Next-Generation Firewall (NGFW) capabilities . . . Fortinet Secure SD-WAN is powered by [a] purpose-build SD-WAN processor." The following excerpt from an April 2020 article from Masergy describes the inclusion of the Fortinet SD-WAN components in the Masergy-Fortinet '593 Products.

The security-driven approach to SD-Branch: Fortinet and Masergy

Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.

SD-WAN with built-in security including next-gen firewalls and advanced routing

- Fortinet Secure SD-WAN with built-in Next-Generation Firewall (NGFW) capabilities offers robust security, connectivity, and management across the branch environment. Fortinet Secure SD-WAN is powered by purpose-built SD-WAN processor, combined with advanced network traffic management functionality such as application steering to ensure high application performance on any WAN link. Fortinet Secure SD-WAN has been recommended twice by NSS Labs consecutively in SD-WAN group tests and trusted by over 21,000 customers.

Extending secure SD-WAN to secure SD-Branch: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge

133. Masergy has directly infringed and continues to directly infringe the '593 patent by, among other things, making, using, offering for sale, and/or selling products and services for processing a flow of a series of information packets.

134. The Masergy-Fortinet '593 Products maintain a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

135. The Masergy-Fortinet '593 Products enable the generation of behavioral statistics based on each packet that is processed.

136. The Masergy-Fortinet '593 Products determine, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

137. The Masergy-Fortinet '593 Products determine whether the flow is exhibiting undesirable behavior regardless of the presence or absence of congestion.

138. The Masergy-Fortinet '593 Products enforce a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

139. By making, using, testing, offering for sale, and/or selling products and services for processing a flow of a series of information packets, including but not limited to the Masergy-Fortinet '593 Products, Masergy has injured Plaintiffs and is liable for directly infringing one or more claims of the '593 patent, including at least claims 25-37, 40, 42, and 44, pursuant to 35 U.S.C. § 271(a).

140. Fortinet indirectly infringes the '593 patent by contributing to the infringement of the '593 patent under 35 U.S.C. § 271(c).

141. Fortinet has had knowledge of the '593 patent since at least June 17, 2020, which is the date the Complaint in *Sable Networks, Inc., et al. v. Fortinet, Inc.*, No. 5:20-cv-00109-RWS (E.D. Tex.), which alleges that Fortinet infringes the '593 patent, was served on Fortinet. Fortinet has known of the '593 patent and its infringement of the '593 patent since at least June 17, 2020.

142. Alternatively, Fortinet has had knowledge of the '593 patent since at least February 7, 2018. On February 7, 2018, Fortinet filed a petition for *Inter Partes* Review of U.S. Patent No. 8,111,629 before the U.S. Patent and Trademark Office's Patent Trial and Appeal Board. *See* IPR2018-00594, Paper 1 (PTAB Feb. 7, 2018). The '775 patent, which is owned by Sable Networks, Inc. was the primary prior art reference analyzed by Fortinet in this *Inter Partes* Review petition. *See* Paper 1 at 26 (identifying the '775 patent either alone or in combination with another reference as "Ground 1" for its argument that the claims of U.S. Patent No. 8,111,629 were invalid). Fortinet then described and analyzed the '775 patent for the next 10 pages of the *Inter Partes* Review petition. *See* Paper 1 at 26-36. On information and belief, Fortinet studied the Sable patent portfolio in connection with its research and preparation of its *Inter Partes* Review

petition seeking the invalidation of U.S. Patent No. 8,111,629. Based upon the extensive analysis of the '775 patent contained in the *Inter Partes* Review petition, on information and belief, Fortinet reviewed each of the patents-in-suit in this case, including the '593 patent, before selecting the '775 patent as Fortinet's primary prior art reference to argue the invalidity of U.S. Patent No. 8,111,629.

143. Fortinet contributes to the infringement of one or more claims of the '593 patent by offering to sell, selling, and/or importing into the United States one or more components of the Masergy-Fortinet '593 Products that constitutes a material part of the invention, knowing that said components are especially made or especially adapted for use in infringing the '593 patent, including at least claims 25-37, 40, 42, and 44, and are not staple articles or commodities of commerce suitable for substantial non-infringing use. The Masergy-Fortinet '593 Products contain Fortinet OS version 6.2 and later, which are programmed with specific software components, *e.g.* FortiGuard Intrusion Prevention System ("IPS") and Fortinet Application Control. These software components, which are incorporated into and sold as part of the Masergy-Fortinet '593 Products, are supplied by Fortinet and are especially made for use in systems that infringe the '593 patent, including at least claims 25-37, 40, 42, and 44, and have no substantial non-infringing uses.

144. The '593 patent is well-known within the industry as demonstrated by multiple citations to the '593 patent in published patents and patent applications assigned to technology companies and academic institutions. Defendants are utilizing the technology claimed in the '593 patent without paying a reasonable royalty. Defendants are infringing the '593 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

145. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '593 patent.

146. As a result of Defendants' infringement of the '593 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 8,817,790

147. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

148. Masergy designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for handling a flow of information packets.

149. Masergy designs, makes, sells, offers to sell, imports, and/or uses devices that enable the identification of a flow based on the behavior of the flow, including at least the Masergy SD-WAN Solution offerings including: Masergy SD-WAN Secure,[42] Masergy Co-Managed SD-WAN,[43] Managed SD-WAN Secure OTT,[44] Masergy SD-WAN Home,[45] Masergy SD-WAN

[42] *Answering Partner FAQs On Managed SD-WAN,* MASERGY DOCUMENTATION (2020) ("Masergy SD-WAN Secure solutions are powered by Fortinet to provide customers with integrated security features such as a next-generation firewall").

[43] *Masergy Expands Its SD-WAN Portfolio Offering the Broadest Choice, Flexibility and Built-In SASE,* MASERGY PRESS RELEASE (July 21, 2020) ("Co-managed solutions: Leveraging the SD-WAN Orchestrator, clients can customize their configurations and make changes while Masergy simultaneously monitors and reports on performance.").

[44] *Masergy Managed SD-WAN Secure OTT*: *Internet Strategies Built For Security and Choice,* MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/managed-sd-wan-secure-ott ("How Masergy's SD-WAN Secure OTT works: Masergy creates an overlay network on top of any public or private network and sends encrypted application traffic via IPsec tunnels to Fortinet-powered endpoints over the public internet ('over the top') for your secure, agile, and scalable corporate network.").

[45] Andy Patrizio, *Masergy teams with Fortinet for at-home SD-WAN*, NETWORKWORLD.COM ARTICLE (October 19, 2020) *available at*: https://www.networkworld.com/article/3586177/masergy-teams-with-fortinet-for-at-home-sd-

Branch solutions,[46] Masergy Secure Access Service Edge solutions (SASE),[47] and Masergy Secure Web Gateway solutions[48] (collectively, the "Masergy-Fortinet '790 Products").

150. The Masergy-Fortinet '790 Products incorporate Fortinet's FortiGate Next-Generation Firewalls and Fortinet SD-WAN devices running Fortinet OS version 5.4 and later. Further, the Masegy-Fortinet '790 Products contain functionality for stateful inspection where the Masergy-Fortinet '790 Products looks at the first packet of a session and perform a lookup in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed. When the first packet of a session is matched in the policy table, stateful inspection adds information about the session to its session table. When subsequent packets are received for the

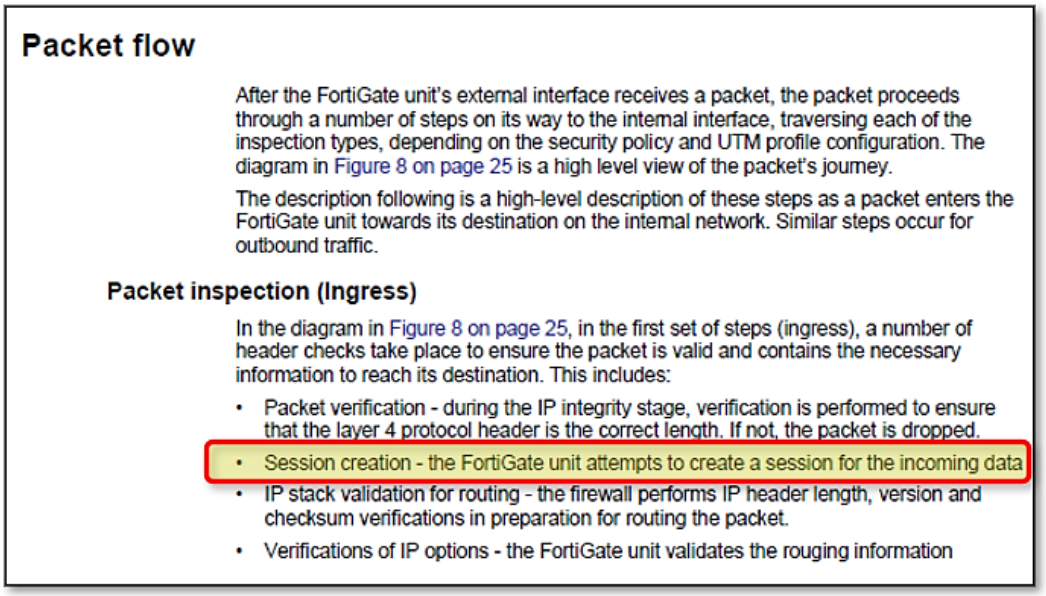
wan.html ("The SD-WAN Secure Home offering utilizes a lightweight Fortinet Secure SD-WAN device for connectivity and improved application performance over a home Internet connection. It also includes built-in next-generation firewall and routing, direct connections to an ecosystem of cloud services").

[46] *Extending secure SD-WAN to secure SD-Branch*: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge ("Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.").

[47] *SASE from Fortinet & Masergy*: *Converging best-of-breed network and security solutions recognized by Gartner,* MASERGY BLOG POSTING (October 6, 2020), *available at*: https://www.masergy.com/blog/sase-from-fortinet-masergy-converging-best-of-breed-network-and-security-solutions-recognized-by-gartner ("Investors seeking out SASE solutions are demanding best-of-breed technologies converged into one solution, and it's here where the Masergy-Fortinet offering stands above the rest.").

[48] *Masergy Secure Web Gateway*, MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/sase/secure-web-gateway ("Masergy's secure web gateway solution is powered by Fortinet . . . Fortinet SWGs go beyond standard web proxies to keep enterprise networks safe from malicious internet traffic, preventing threats from entering the network and causing an infection or intrusion.").

same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table).



Packet flow

After the FortiGate unit's external interface receives a packet, the packet proceeds through a number of steps on its way to the internal interface, traversing each of the inspection types, depending on the security policy and UTM profile configuration. The diagram in Figure 8 on page 25 is a high level view of the packet's journey.

The description following is a high-level description of these steps as a packet enters the FortiGate unit towards its destination on the internal network. Similar steps occur for outbound traffic.

Packet inspection (Ingress)

In the diagram in Figure 8 on page 25, in the first set of steps (ingress), a number of header checks take place to ensure the packet is valid and contains the necessary information to reach its destination. This includes:

- Packet verification - during the IP integrity stage, verification is performed to ensure that the layer 4 protocol header is the correct length. If not, the packet is dropped.
- Session creation - the FortiGate unit attempts to create a session for the incoming data
- IP stack validation for routing - the firewall performs IP header length, version and checksum verifications in preparation for routing the packet.
- Verifications of IP options - the FortiGate unit validates the rouging information

FortiGate Fundamentals, FORTIOS HANDBOOK V3 FOR FORTIOS 4.0 MR3 at 24 (June 2011) (emphasis added).

151. The Masergy-Fortinet '790 Products comprise endpoint hardware that comprises a router with a network interface.

> Unlike other providers, our Managed SD-WAN solutions enable you to leverage SD-WAN at some locations without having to deploy it everywhere in a "mix and match" WAN design approach. Masergy SD-WAN endpoint hardware is provided by our partners at Fortinet with an embedded router, firewall, and unified threat management (UTM) capabilities. Combined with our managed software-defined network backbone, these features enable companies to install secure Managed SD-WAN connections quickly and safely on their network edge that extends to both public and private cloud assets.

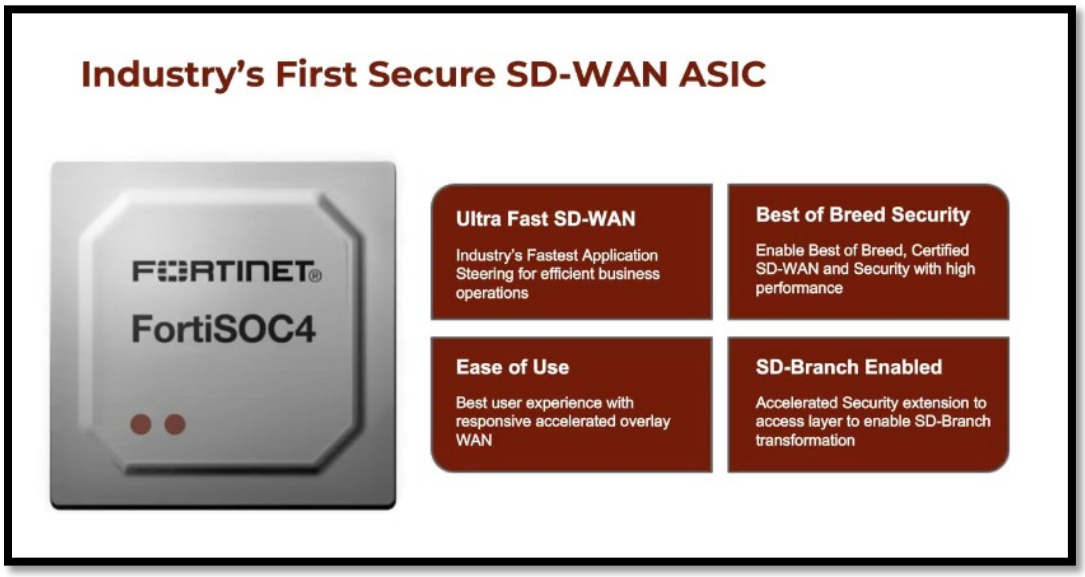
Masergy: *Your SD-WAN questions answered,* MASERGY WEBSITE (last visited December 2020); *available at*: https://www.masergy.com/faq/managed-sd-wan (emphasis added).

152. The Masergy-Fortinet '790 Products include Fortinet's Application-Specific Integrated Circuits (ASIC). The ASIC chips are purpose-built by Fortinet for SD-WAN solutions. The following excerpt from a Masergy article describes the incorporation of the Fortinet ASIC in the Masergy-Fortinet '790 Products.

> Best-of-Breed SD-WAN & Security: Fortinet is committed to driving a consistent security posture from the WAN edge to both data centers and multi-cloud environments by natively integrating security functions, including NGFW, IPS, anti-virus, anti-malware, web filtering, SSL inspection (including TLS 1.3), and sandboxing. Fortinet also provides an integrated CASB service to protect SaaS applications and traffic and to prevent problems related to Shadow IT. Our patented innovation of a purpose-built SD-WAN ASIC enables faster Application Steering, Multi-Path Intelligence, and WAN Path Remediation with forward error correction (FEC) to overcome adverse WAN conditions.

Fortinet & Masergy: *The security-driven approach to SD-WAN*, MASERGY BLOG POSTING (January 16, 2020) *available at*: https://www.masergy.com/blog/fortinet-masergy-the-security-driven-approach-to-sd-wan (emphasis added).

153. A recent joint webcast conducted by Masergy and Fortinet identified that the Masergy-Fortinet '790 Products include a secure SD-WAN ASIC developed by Fortinet. The following excerpt from the webcast shows the functionality of the FortiSOC4 ASIC that is included in the Masergy-Fortinet '790 Products.



Enabling Enterprises with Secure, Agile and Intelligent Managed SD-WAN, Masergy-FORTINET PARTNER WEBCAST (April 29, 2020), *available at*: https://www.fortinet.com/resources-campaign/network

154. The Masergy-Fortinet '790 Products include Fortinet's SD-WAN devices. Specifically, a February 2020 press release from Fortinet quoted Masergy's Executive Vice

President, Bob Laskey, as describing the Masergy-Fortinet '790 Products as built on "Fortinet's Secure SD-WAN" components.

> Built on Fortinet's Secure SD-WAN, Masergy's Managed SD-WAN solution gives clients software-defined network services and three tiered options for managed security services. It's a winning combination that resonates with global enterprises needing cloud application performance, 24/7 threat monitoring, as well as incident response. Like Fortinet, we believe networking and security need to be inextricably tied, and resellers with a Fortinet-Masergy partnership address more needs across both IT domains.

Fortinet Drives Channel Business Opportunities with Secure SD-WAN, FORTINET PRESS RELEASE (February 5, 2020) (quote from Bob Laskey, Executive VP at Masergy).

155. The Masergy-Fortinet '790 Products include FortiGate devices that contain functionality for SD-WAN, routing, and next-generation firewall protection. The integration of Fortinet's FortiGate devices into the Masergy-Fortinet '790 Products enables the products to infringe the '790 patent. The following excerpt from documentation of the Masergy-Fortinet '790 Products states that Masergy delivers secure SD-WAN solutions using a Fortinet FortiGate hardware endpoint.

Managed SD-WAN by Masergy

As a 20-year pioneer in software-defined networking, Masergy is a leading managed services provider delivering SD-WAN, unified communications, and managed security solutions to global enterprises.

Masergy delivers secure SD-WAN solutions to customers using a customized Fortinet FortiGate hardware endpoint. The customized FortiGate device is pre-provisioned with features including SD-WAN, routing, next-generation firewall (with options for additional unified threat management protection, 24/7 threat monitoring and incident response, and more); and enables the addition of secure LAN switching and secure Wi-Fi, all with centralized policy management.

While Masergy can ship out a small appliance for critical or power remote users to extend full functionality of SD-WAN features, remote users can also connect to Masergy's global network and cloud platform via VPNs. Businesses can seamlessly deploy remote VPN connections due to the software-defined networking (SDN) elements built into Masergy's network. The SDN-enabled platform ensures fast and easy deployment and disconnection of connections, tunnels, links, loops, and bandwidth, compared to legacy networks governed by manual processes.

Roopa Honnachari, *COVID-19 Highlights the Business Case for Extending SD-WAN to Remote Workers,* BUSINESS COMMUNICATION SERVICES (BCS) VOL. 14 NO. 1 at 8 (May 2020) (emphasis added).

156. The Masergy-Fortinet '790 Products incorporate Fortinet's FortiGate Next Generation Firewall and SD-WAN products. A November 2020 article describing the Masergy-Fortinet '790 Products stated that Masergy combined Fortinet's FortiGate Next Generation Firewall and SD-WAN components into a "single platform."

> Masergy has bulked up its own SD-WAN Secure solution to make a bigger play into the SASE space by expanding cloud firewalls into all of its global points-of-presence (POPs). Masergy announced on Monday that it had integrated Fortinet's FortiGate Next-Generation Firewalls integrate NGFW and SD-WAN capabilities onto a single platform and deployed them in all of its software-defined network POPs as well as integrated them into its SD-WAN and security policies.

Mike Robuck, *Masergy goes bigger and bolder into SASE arena by taking best-of-breed approach,* FIERCETELECOM.COM ARTICLE (November 16, 2020), *available at*: https://www.fiercetelecom.com/telecom/masergy-goes-bigger-and-bolder-into-sase-arena (emphasis added).

157. The Masergy-Fortinet '790 Products include Fortinet's Secure SD-WAN with "built-in Next-Generation Firewall (NGFW) capabilities . . . Fortinet Secure SD-WAN is powered by [a] purpose-build SD-WAN processor." The following excerpt from an April 2020 article from Masergy describes the inclusion of the Fortinet SD-WAN components in the Masergy-Fortinet '790 Products.

The security-driven approach to SD-Branch: Fortinet and Masergy

Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.

SD-WAN with built-in security including next-gen firewalls and advanced routing

- Fortinet Secure SD-WAN with built-in Next-Generation Firewall (NGFW) capabilities offers robust security, connectivity, and management across the branch environment. Fortinet Secure SD-WAN is powered by purpose-built SD-WAN processor, combined with advanced network traffic management functionality such as application steering to ensure high application performance on any WAN link. Fortinet Secure SD-WAN has been recommended twice by NSS Labs consecutively in SD-WAN group tests and trusted by over 21,000 customers.

Extending secure SD-WAN to secure SD-Branch: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge

158. One or more of the Masergy-Fortinet '790 Products include technology for handling a flow of information packets. Specifically, the Masergy-Fortinet '790 Product process information packets that have the same header information.

159. The Masergy-Fortinet '790 Products are available to businesses and individuals throughout the United States.

160. The Masergy-Fortinet '790 Products are provided to businesses and individuals located in the Eastern District of Texas.

161. Masergy has directly infringed and continues to directly infringe the '790 patent by, among other things, making, using, offering for sale, and/or selling technology for handling a flow of information packets, including but not limited to the Masergy-Fortinet '790 Products.

162. The Masergy-Fortinet '790 Products process a flow comprised of two or more information packets having header information in common. Further, the Masergy-Fortinet '790

Products use header-independent statistics for traffic classification. These statistics include bit rate, packet counts, and byte counts that are used to identify a particular traffic type.

163. The Masergy-Fortinet '790 Products store header-independent statistics about the flow in a flow block associated with the flow.

164. The Masergy-Fortinet '790 Products perform traffic matching using header-independent statistics such as: total number of input packets, total number of output packets, input bit rates, and output bit rates.

165. The Masergy-Fortinet '790 Products update the header-independent statistics in the flow block as each information packet belonging to the flow is processed. The header-independent statistics are stored in a flow block associated with the flow.

166. The Masergy-Fortinet '790 Products categorize the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type.

167. The Masergy-Fortinet '790 Products perform an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

168. By making, using, testing, offering for sale, and/or selling products and services, including but not limited to the Masergy-Fortinet '790 Products, Masergy has injured Plaintiffs and is liable for directly infringing one or more claims of the '790 patent, including at least claims 28 and 29, pursuant to 35 U.S.C. § 271(a).

169. Fortinet indirectly infringes the '790 patent by contributing to the infringement of the '790 patent under 35 U.S.C. § 271(c).

170. Fortinet has had knowledge of the '790 patent since at least June 17, 2020, which is the date the Complaint in *Sable Networks, Inc., et al. v. Fortinet, Inc.*, No. 5:20-cv-00109-RWS (E.D. Tex.), which alleges that Fortinet infringes the '790 patent, was served on Fortinet. Fortinet has known of the '790 patent and its infringement of the '790 patent since at least June 17, 2020.

171. Alternatively, Fortinet has had knowledge of the '790 patent since at least February 7, 2018. On February 7, 2018, Fortinet filed a petition for *Inter Partes* Review of U.S. Patent No. 8,111,629 before the U.S. Patent and Trademark Office's Patent Trial and Appeal Board. *See* IPR2018-00594, Paper 1 (PTAB Feb. 7, 2018). The '775 patent, which is owned by Sable Networks, Inc. was the primary prior art reference analyzed by Fortinet in this *Inter Partes* Review petition. *See* Paper 1 at 26 (identifying the '775 patent either alone or in combination with another reference as "Ground 1" for its argument that the claims of U.S. Patent No. 8,111,629 were invalid). Fortinet then described and analyzed the '775 patent for the next 10 pages of the *Inter Partes* Review petition. *See* Paper 1 at 26-36. On information and belief, Fortinet studied the Sable patent portfolio in connection with its research and preparation of its *Inter Partes* Review petition seeking the invalidation of U.S. Patent No. 8,111,629. Based upon the extensive analysis of the '775 patent contained in the *Inter Partes* Review petition, on information and belief, Fortinet reviewed each of the patents-in-suit in this case, including the '790 patent, before selecting the '775 patent as Fortinet's primary prior art reference to argue the invalidity of U.S. Patent No. 8,111,629.

172. Fortinet contributes to the infringement of one or more claims of the '790 patent by offering to sell, selling, and/or importing into the United States one or more components of the Masergy-Fortinet '790 Products that constitutes a material part of the invention, knowing that said components are especially made or especially adapted for use in infringing the '790 patent,

including at least claims 28 and 29, and are not staple articles or commodities of commerce suitable for substantial non-infringing use. The Masergy-Fortinet '790 Products contain Fortinet OS version 5.4 and later, which are programmed with specific software components, *e.g.* Fortinet Stateful Inspection and/or Fortinet Application Control. These software components, which are incorporated into and sold as part of the Masergy-Fortinet '790 Products, are supplied by Fortinet and are especially made for use in systems that infringe the '790 patent, including at least claims 28 and 29, and have no substantial non-infringing uses.

173. The '790 patent is well-known within the industry as demonstrated by multiple citations to the '790 patent in published patents and patent applications assigned to technology companies and academic institutions. Defendants are utilizing the technology claimed in the '790 patent without paying a reasonable royalty. Defendants are infringing the '790 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

174. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '790 patent.

175. As a result of Defendants' infringement of the '790 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 9,774,501

176. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

177. Masergy designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for detecting outlier users of a network resource.

178. Masergy designs, makes, sells, offers to sell, imports, and/or uses the Masergy SD-WAN Solution offerings including at least the following product offerings: Masergy SD-WAN Secure,[49] Masergy Co-Managed SD-WAN,[50] Managed SD-WAN Secure OTT,[51] Masergy SD-WAN Home,[52] Masergy SD-WAN Branch solutions,[53] Masergy Secure Access Service Edge

[49] *Answering Partner FAQs On Managed SD-WAN,* MASERGY DOCUMENTATION (2020) ("Masergy SD-WAN Secure solutions are powered by Fortinet to provide customers with integrated security features such as a next-generation firewall").

[50] *Masergy Expands Its SD-WAN Portfolio Offering the Broadest Choice, Flexibility and Built-In SASE,* MASERGY PRESS RELEASE (July 21, 2020) ("Co-managed solutions: Leveraging the SD-WAN Orchestrator, clients can customize their configurations and make changes while Masergy simultaneously monitors and reports on performance.").

[51] *Masergy Managed SD-WAN Secure OTT*: *Internet Strategies Built For Security and Choice,* MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/managed-sd-wan-secure-ott ("How Masergy's SD-WAN Secure OTT works: Masergy creates an overlay network on top of any public or private network and sends encrypted application traffic via IPsec tunnels to Fortinet-powered endpoints over the public internet ('over the top') for your secure, agile, and scalable corporate network.").

[52] Andy Patrizio, *Masergy teams with Fortinet for at-home SD-WAN*, NETWORKWORLD.COM ARTICLE (October 19, 2020) *available at*: https://www.networkworld.com/article/3586177/masergy-teams-with-fortinet-for-at-home-sd-wan.html ("The SD-WAN Secure Home offering utilizes a lightweight Fortinet Secure SD-WAN device for connectivity and improved application performance over a home Internet connection. It also includes built-in next-generation firewall and routing, direct connections to an ecosystem of cloud services").

[53] *Extending secure SD-WAN to secure SD-Branch*: *The convergence of WAN and LAN at the edge*, MASERGY BLOG POST (April 23, 2020), *available at*: https://www.masergy.com/blog/extending-secure-sd-wan-to-secure-sd-branch-the-convergence-of-wan-and-lan-at-the-edge ("Masergy and Fortinet have partnered together to provide security-driven SD-Branch solutions for global enterprises. SD-Branch solutions pair Fortinet's edge devices and security features with fully managed SD-WAN services from Masergy.").

solutions (SASE),[54] and Masergy Secure Web Gateway solutions[55] (collectively, the "Masergy-Fortinet '501 Products").

179. The Masergy-Fortinet '501 Products incorporate Fortinet components running Fortinet OS version 6.0 and later including Fortinet's FortiGate Next-Generation Firewalls.

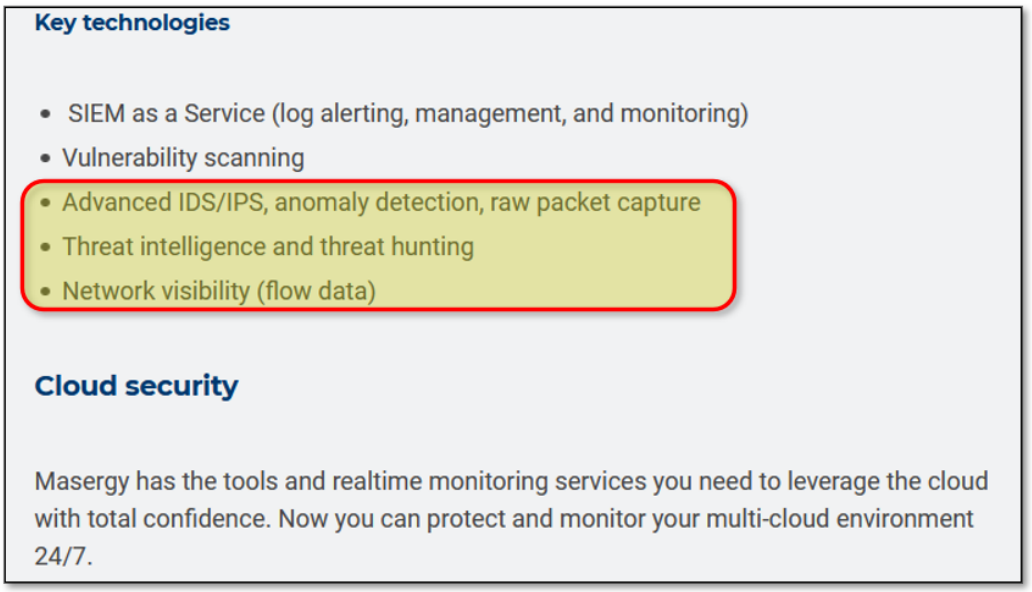
> Details of the Masergy SASE offering are as follows: Cloud firewalls in all global points of presence (POPs) powered by Fortinet: Masergy has a number of global POPs where it will offer cloud resident firewalls using Fortinet's FortiGate next-generation firewall (NGFW). Cloud firewalls are fast and easy to deploy and provide corporate-class threat protection to sites that are as small as a single person. It's important to note that Masergy will continue to offer its edge-based service for users that prefer an on-premises appliance. This hybrid approach provides customers with threat protection where they want it, without the associated complexity of managing a highly distributed environment.

Zeus Kerravala, *How Masergy Uses Partners to Provide Secure-Access Service Edge*, EWEEK.COM ARTICLE (November 16, 2020), *available at*: https://www.eweek.com/security/how-masergy-uses-partners-for-secure-access-service-edge (emphasis added).

180. The Masergy-Fortinet '501 Products perform the method of monitoring stream data associated with a user or device's usage of a network resource for a predetermined time. The monitoring of stream data associated with a user is conducted by the Masergy-Fortinet '501 Products using components supplied by Fortinet. For example, the Masergy-Fortinet '501 Products enable "Advanced IDS/IPS, anomaly detection, raw packet capture."

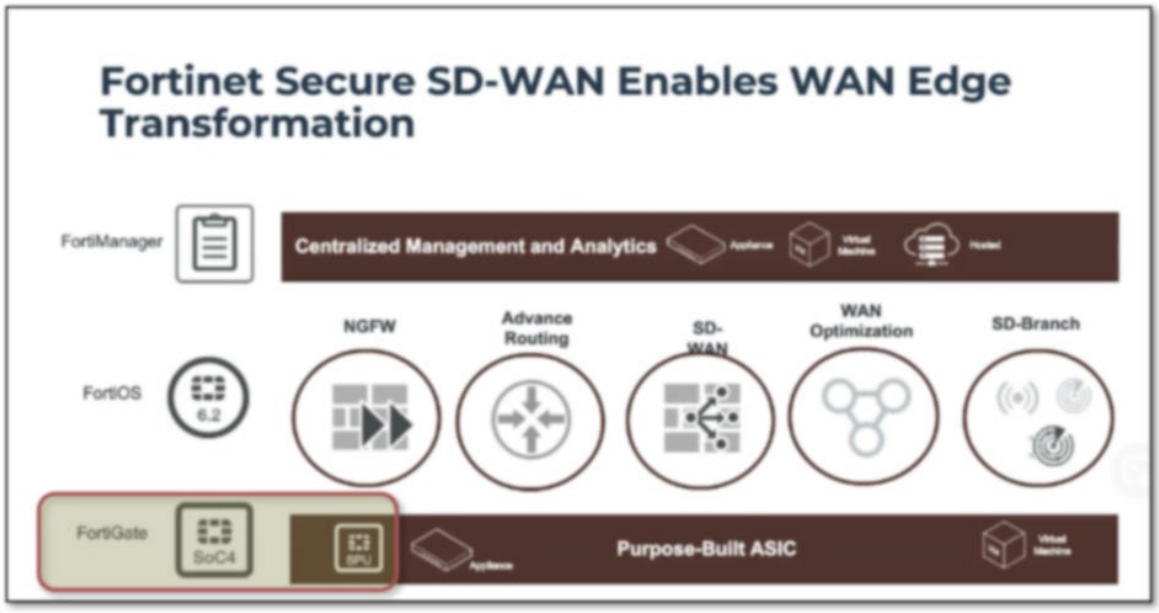
[54] *SASE from Fortinet & Masergy*: *Converging best-of-breed network and security solutions recognized by Gartner,* MASERGY BLOG POSTING (October 6, 2020), *available at*: https://www.masergy.com/blog/sase-from-fortinet-masergy-converging-best-of-breed-network-and-security-solutions-recognized-by-gartner ("Investors seeking out SASE solutions are demanding best-of-breed technologies converged into one solution, and it's here where the Masergy-Fortinet offering stands above the rest.").

[55] *Masergy Secure Web Gateway*, MASERGY WEBSITE (last visited December 2020), *available at*: https://www.masergy.com/sd-wan/sase/secure-web-gateway ("Masergy's secure web gateway solution is powered by Fortinet . . . Fortinet SWGs go beyond standard web proxies to keep enterprise networks safe from malicious internet traffic, preventing threats from entering the network and causing an infection or intrusion.").



Masergy Managed Security Solution Brief, MASERGY.COM DOCUMENTATION (last visited December 2020), *available at*: https://www.masergy.com/solution-brief/managed-security (emphasis added).

181. The Masergy-Fortinet '501 Products perform the step of deriving a flow-count history. The flow-count history is generated based on stream data where a flow is a connection between a source IP address and a transport layer port to a destination IP address and transport layer port in which all of the packets use the same protocol. To perform this step the Masergy-Fortinet '501 Products use the Fortinet-provided application-specific integrated circuit ("ASIC") components. The following excerpt from a Masergy and Fortinet joint webcast describes the use of the FortiGate SOC4 and SPU ASICs to perform centralized management and analytics.



Enabling Enterprises with Secure, Agile and Intelligent Managed SD-WAN, Masergy-FORTINET PARTNER WEBCAST (April 29, 2020), *available at*: https://www.fortinet.com/resources-campaign/network (annotation added).

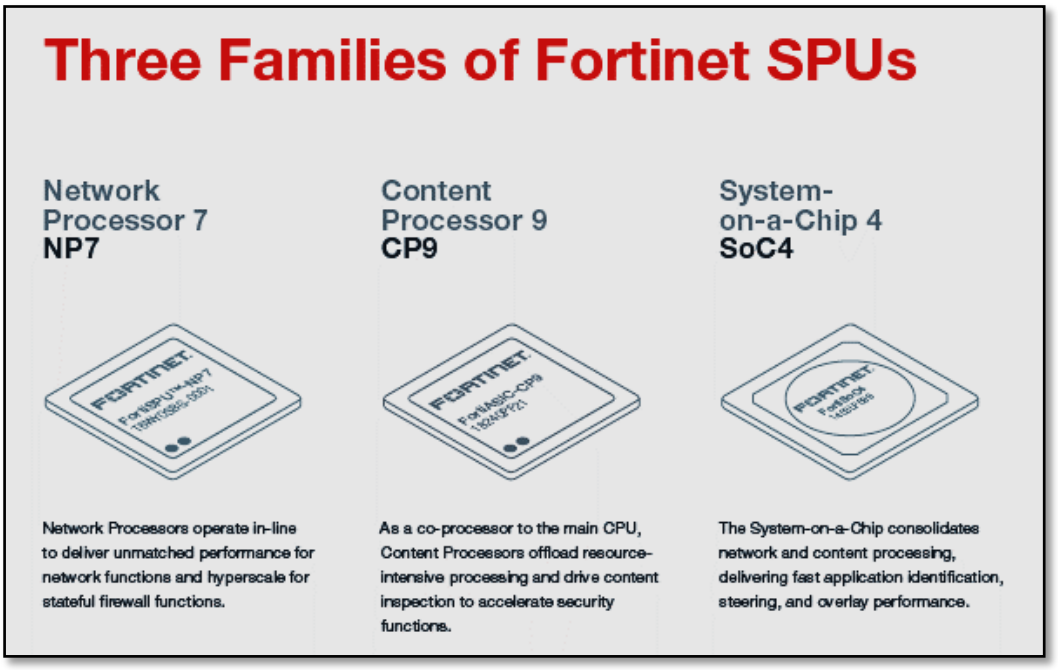
182. The Masergy-Fortinet '501 Products perform the step of applying an outlier detection algorithm to the generated flow-count history associated with a user or a device and comparing the flow-count history to flow-count histories associated with other users or devices on the network. This step is performed in part by the ASIC chips that are provided by Fortinet and incorporated in the Masergy-Fortinet '501 Products. The Fortinet ASIC chips are purpose-built by Fortinet for SD-WAN solutions such as the Masergy-Fortinet '501 Products. The following excerpt from a Masergy article describes the incorporation of the Fortinet ASIC in the Masergy-Fortinet '501 Products.

> Fortinet is committed to driving a consistent security posture from the WAN edge to both data centers and multi-cloud environments by natively integrating security functions, including NGFW, IPS, anti-virus, anti-malware, web filtering, SSL inspection (including TLS 1.3), and sandboxing. Fortinet also provides an integrated CASB service to protect SaaS applications and traffic and to prevent problems related to Shadow IT. Our patented innovation of a purpose-built SD-WAN ASIC enables faster Application Steering, Multi-Path Intelligence, and

WAN Path Remediation with forward error correction (FEC) to overcome adverse WAN conditions.

Fortinet & Masergy: *The security-driven approach to SD-WAN*, MASERGY BLOG POSTING (January 16, 2020), *available at*: https://www.masergy.com/blog/fortinet-masergy-the-security-driven-approach-to-sd-wan (emphasis added).

183. Fortinet has identified that its ASIC components including the ASICs that are incorporated into the Masergy-Fortinet '501 Products perform network and content processing, application identification, steering and overlay performance. The following excerpt from Fortinet documentation shows the functionality of the FortiSOC4 ASIC that is included in the Masergy-Fortinet '501 Products.



Fortinet Security Processing Units: Engineered for Innovation, FORTINET SPU BROCHURE AT 3 (January 2020).

184. The Masergy-Fortinet '501 Products assign a flow-count band to the user based on the outlier detection algorithm and flow-count history. The method of assigning a flow-count band to a user based on the user's flow-count history is performed using Fortinet components that are incorporated into the Masergy-Fortinet '501 Products. A February 2020 press release from

Fortinet quotes Masergy's Executive Vice President, Bob Laskey, describing the Masergy-Fortinet '501 Products as built on "Fortinet's Secure SD-WAN" components.

> Built on Fortinet's Secure SD-WAN, Masergy's Managed SD-WAN solution gives clients software-defined network services and three tiered options for managed security services. It's a winning combination that resonates with global enterprises needing cloud application performance, 24/7 threat monitoring, as well as incident response.

Fortinet Drives Channel Business Opportunities with Secure SD-WAN, FORTINET PRESS RELEASE (February 5, 2020) (quote from Bob Laskey, Masergy Executive Vice President) (emphasis added).

185. The Masergy-Fortinet '501 Products include Fortinet components that contain functionality for SD-WAN, routing, and next-generation firewall protection. The integration of Fortinet's FortiGate components into the Masergy-Fortinet '501 Products enables the Masergy-Fortinet '501 Products to infringe the '501 patent claims, including through comprising functionality for a bulk statistics record module. The following excerpt from documentation of the Masergy-Fortinet '501 Products states that Masergy delivers secure SD-WAN solutions using a Fortinet FortiGate hardware endpoint.

Managed SD-WAN by Masergy

As a 20-year pioneer in software-defined networking, Masergy is a leading managed services provider delivering SD-WAN, unified communications, and managed security solutions to global enterprises.

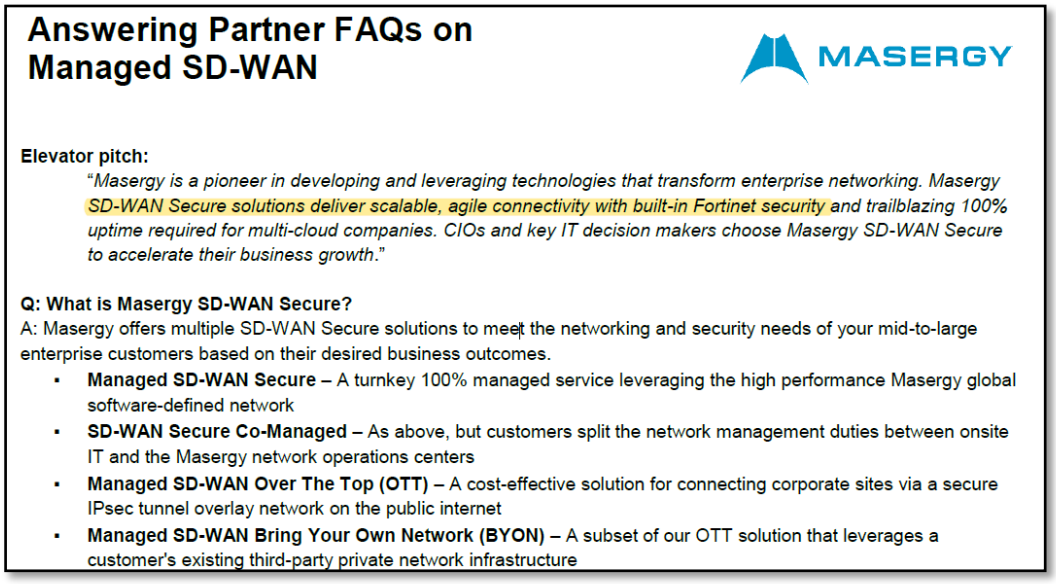
Masergy delivers secure SD-WAN solutions to customers using a customized Fortinet FortiGate hardware endpoint. The customized FortiGate device is pre-provisioned with features including SD-WAN, routing, next-generation firewall (with options for additional unified threat management protection, 24/7 threat monitoring and incident response, and more); and enables the addition of secure LAN switching and secure Wi-Fi, all with centralized policy management.

Roopa Honnachari, *COVID-19 Highlights the Business Case for Extending SD-WAN to Remote Workers,* BUSINESS COMMUNICATION SERVICES (BCS) VOL. 14 NO. 1 at 8 (May 2020) (emphasis added).

186. The Masergy-Fortinet '501 Products incorporate Fortinet's FortiGate Next Generation Firewall and SD-WAN components. A November 2020 article describing the Masergy-Fortinet '501 Products stated that Masergy combined Fortinet's FortiGate Next

Generation Firewall and SD-WAN components into a "single platform." "Masergy has bulked up its own SD-WAN Secure solution to make a bigger play into the SASE space by expanding cloud firewalls into all of its global points-of-presence (POPs). Masergy announced on Monday that it had integrated Fortinet's FortiGate Next-Generation Firewalls integrate NGFW and SD-WAN capabilities onto a single platform and deployed them in all of its software-defined network POPs as well as integrated them into its SD-WAN and security policies." Mike Robuck, *Masergy goes bigger and bolder into SASE arena by taking best-of-breed approach,* FIERCETELECOM.COM ARTICLE (November 16, 2020), *available at*: https://www.fiercetelecom.com/telecom/masergy-goes-bigger-and-bolder-into-sase-arena (emphasis added).

187. The Masergy-Fortinet '501 Products include "built-in Fortinet security." The following excerpt from a July 2020 Partner FAQ authored by Masergy describes the inclusion of the Fortinet SD-WAN components in the Masergy-Fortinet '501 Products.



Answering Partner FAQs on Managed SD-WAN

MASERGY

Elevator pitch:

"*Masergy is a pioneer in developing and leveraging technologies that transform enterprise networking. Masergy SD-WAN Secure solutions deliver scalable, agile connectivity with built-in Fortinet security and trailblazing 100% uptime required for multi-cloud companies. CIOs and key IT decision makers choose Masergy SD-WAN Secure to accelerate their business growth.*"

Q: What is Masergy SD-WAN Secure?

A: Masergy offers multiple SD-WAN Secure solutions to meet the networking and security needs of your mid-to-large enterprise customers based on their desired business outcomes.

- **Managed SD-WAN Secure** – A turnkey 100% managed service leveraging the high performance Masergy global software-defined network
- **SD-WAN Secure Co-Managed** – As above, but customers split the network management duties between onsite IT and the Masergy network operations centers
- **Managed SD-WAN Over The Top (OTT)** – A cost-effective solution for connecting corporate sites via a secure IPsec tunnel overlay network on the public internet
- **Managed SD-WAN Bring Your Own Network (BYON)** – A subset of our OTT solution that leverages a customer's existing third-party private network infrastructure

Answering Partner FAQs On Managed SD-WAN, MASERGY DOCUMENTATION at 1 (July 21, 2020) (emphasis added).

188. One or more of the Masergy-Fortinet '501 Products include technology for tracking flow data of a user subscriber, for a predetermined time interval.

189. One or more of the Masergy-Fortinet '501 Products include functionality for aggregating flow data of a user for a number of time periods. The flow data that is aggregated by the Masergy-Fortinet '501 Products includes network communications between a particular source IP address and transport layer port to a particular destination IP address and transport layer port in which all of the packets are using the same protocol.

190. One or more of the Masergy-Fortinet '501 Products generate a flow-count pattern where the flow-count pattern is the count of the number of flows the user initiates as either the source IP address or destination IP address during a predetermined time period.

191. One or more of the Masergy-Fortinet '501 Products apply an outlier detection logic (algorithm) to the flow-count pattern as compared to a plurality of other flow-count patterns associated with a plurality of other users.

192. One or more of the Masergy-Fortinet '501 Products assign a flow-count band to the user or device based on a first result of the outlier detection logic.

193. One or more of the Masergy-Fortinet '501 Products apply a mitigating action to the user concerning the user's access to the network resource based on the flow-count band assigned.

194. The Masergy-Fortinet '501 Products are available to businesses and individuals throughout the United States.

195. The Masergy-Fortinet '501 Products are provided to businesses and individuals located in the Eastern District of Texas.

196. Masergy has directly infringed and continues to directly infringe the '501 patent by, among other things, making, using, offering for sale, and/or selling technology for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Masergy-Fortinet '501 Products.

197. By making, using, testing, offering for sale, and/or selling products and services for detecting outlier users of a network resource, including but not limited to the Masergy-Fortinet '501 Products, Masergy has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '501 patent, including at least claims 1, 2, 6, 7, 10, 11, 14, 15, and 18-20 pursuant to 35 U.S.C. § 271(a).

198. Fortinet indirectly infringes the '501 patent, including at least claims 1, 2, 6, 7, and 18-20 by actively inducing infringement under 35 U.S.C. § 271(b).

199. Fortinet has had knowledge of the '501 patent since at least service of this Complaint or shortly thereafter, and Fortinet knew of the '501 patent and knew of its infringement, including by way of this lawsuit.

200. Alternatively, Fortinet has had knowledge of the '501 patent since at least November 9, 2020, or shortly thereafter. On November 9, 2020, Sable Networks, Inc. and Sable IP, LLC produced the Sable Networks-Sable IP Patent Exclusive License Agreement at SBL-VNU_0000001-SBL-VNU_0000008 in the *Sable Networks, Inc., et al. v. Fortinet, Inc.*, No. 5:20-cv-00109-RWS (E.D. Tex.) action currently pending in this District. The Sable Networks-Sable IP Patent Exclusive License Agreement identifies the '501 patent and was produced to Fortinet.

201. Alternatively, Fortinet has had knowledge of the '501 patent since at least February 7, 2018. On February 7, 2018, Fortinet filed a petition for *Inter Partes* Review of U.S. Patent No. 8,111,629 before the U.S. Patent and Trademark Office's Patent Trial and Appeal Board. *See* IPR2018-00594, Paper 1 (PTAB Feb. 7, 2018). U.S. Patent No. 8,085,775 (the "'775 patent"), which is owned by Sable Networks, Inc. was the primary prior art reference analyzed by Fortinet in this *Inter Partes* Review petition. *See* Paper 1 at 26 (identifying the '775 patent either alone or in combination with another reference as "Ground 1" for its argument that the claims of U.S. Patent

No. 8,111,629 were invalid). Fortinet then described and analyzed the '775 patent for the next 10 pages of the *Inter Partes* Review petition. *See* Paper 1 at 26-36. On information and belief, Fortinet studied the Sable patent portfolio, which includes the '775 patent in addition to each of the patents-in-suit in this action, in connection with its research and preparation of its *Inter Partes* Review petition seeking the invalidation of U.S. Patent No. 8,111,629. Based upon the extensive analysis of the '775 patent contained in the *Inter Partes* Review petition, on information and belief, Fortinet reviewed each of the patents-in-suit in this case, including the '501 patent, before selecting the '775 patent as Fortinet's primary prior art reference to argue the invalidity of U.S. Patent No. 8,111,629.

202. Fortinet intended to induce patent infringement by third-party customers and users of the Masergy-Fortinet '501 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Fortinet specifically intended and was aware that the normal and customary use of the accused products would infringe the '501 patent. Fortinet performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '501 patent and with the knowledge that the induced acts would constitute infringement. For example, Fortinet provides the Masergy-Fortinet '501 Products that have the capability of operating in a manner that infringe one or more of the claims of the '501 patent, including at least claims 1, 2, 6, 7, and 18-20, and Fortinet further provides documentation and training materials that cause customers and end users of the Masergy-Fortinet '501 Products to utilize the products in a manner that directly infringe one or more claims of the '501 patent.[56] By providing instruction and training to

[56] *See e.g., Fortinet Drives Channel Business Opportunities with Secure SD-WAN*, FORTINET PRESS RELEASE (February 5, 2020); *Fortinet Customer Profile*: *Masergy - Partnering with Fortinet to Deliver a Security-Driven Approach to SD-WAN and SD-Branch*, FORTINET.COM WEBSITE (last visited December 2020), *available at*:

customers and end-users on how to use the Masergy-Fortinet '501 Products in a manner that directly infringes one or more claims of the '501 patent, including at least claims 1, 2, 6, 7, and 18-20, Fortinet specifically intended to induce infringement of the '501 patent. Fortinet engaged in such inducement to promote the sales of the Masergy-Fortinet '501 Products, e.g., through Fortinet user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '501 patent. Accordingly, Fortinet has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '501 patent, knowing that such use constitutes infringement of the '501 patent.

203. Fortinet also indirectly infringes the '501 patent by contributing to the infringement of the '501 patent under 35 U.S.C. § 271(c).

204. Fortinet contributes to the infringement of one or more claims of the '501 patent by offering to sell, selling, and/or importing into the United States one or more components of the Masergy-Fortinet '501 Products that constitutes a material part of the invention, knowing that said components are especially made or especially adapted for use in infringing the '501 patent, including at least claims 10, 11, 14, and 15, and are not staple articles or commodities of commerce suitable for substantial non-infringing use. The Masergy-Fortinet '501 Products are programmed with specific software components, *e.g.*, Fortinet SD-WAN NGFW and Fortinet SD-WAN ASIC.

---

https://www.fortinet.com/customers/masergy; *Enabling Enterprises with Secure, Agile and Intelligent Managed SD-WAN*, MASERGY-FORTINET PARTNER WEBCAST (April 29, 2020), *available at*: https://www.fortinet.com/resources-campaign/network; *Driving Growth, Security, and Business Efficiency with Managed SD-WAN Services*, FORTINET PARTNER WEBCAST (September 16, 2020), *available at*: https://events.fortinet.com/WeeklyWebinarSeries/session/32051 (joint webcast hosted by Fortinet featuring speakers from Masergy and Fortinet); FORTICLIENT - ADMINISTRATION GUIDE VERSION 6.4.1 (August 24, 2020); *Fortinet Secure SD-WAN Reference Architecture,* FORTINET WHITE PAPER (April 3, 2019); FORTIOS HANDBOOK - PARALLEL PATH PROCESSING (LIFE OF A PACKET) VERSION 5.6.7 (March 15, 2019); and FORTIOS – COOKBOOK VERSION 6.2.4 (June 1, 2020).

These software components, which are incorporated into and sold as part of the Masergy-Fortinet '501 Products, are supplied by Fortinet and are especially made for use in systems that infringe the '501 patent, including at least claims 10, 11, 14, and 15, and have no substantial non-infringing uses.

205. The '501 patent is well-known within the industry as demonstrated by multiple citations to the '501 patent in published patents and patent applications assigned to technology companies and academic institutions. Defendants are utilizing the technology claimed in the '501 patent without paying a reasonable royalty. Defendants are infringing the '501 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

206. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '501 patent.

207. As a result of Defendants' infringement of the '501 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Sable IP, LLC and Sable Networks, Inc. respectfully request that this Court enter:

A. A judgment in favor of Plaintiffs that Masergy has directly infringed, either literally and/or under the doctrine of equivalents, the '431, '593, '790, and/or '501 patents;

B. A judgment in favor of Plaintiffs that Fortinet has indirectly infringed the '431, '593, '790, and/or '501 patents;

C. An award of damages resulting from Defendants' acts of infringement in accordance with 35 U.S.C. § 284;

D. A judgment and order finding that Defendants' infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiffs enhanced damages.

E. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiffs their reasonable attorneys' fees against Defendants.

F. Any and all other relief to which Plaintiffs may show themselves to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Sable IP, LLC and Sable Networks, Inc. request a trial by jury of any issues so triable by right.

Dated: December 10, 2020

Respectfully submitted,

/s/ Daniel P. Hipskind

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com

Attorneys for Sable Networks, Inc. and Sable IP, LLC