BAKER BOTTS L.L.P.
Kurt M. Pankratz (SBN 24013291) (*Pro Hac Vice*)
kurt.pankratz@bakerbotts.com
Chad C. Walters (SBN 24034730) (*Pro Hac Vice*)
chad.walters@bakerbotts.com
James Williams (SBN 24075284) (*Pro Hac Vice*)
james.williams@bakerbotts.com
Harrison Rich (SBN 24083730) (*Pro Hac Vice*)
harrison.rich@bakerbotts.com
Clarke Stavinoha (SBN 24093198) *(Pro Hac Vice)*
clarke.stavinoha@bakerbotts.com
Morgan Grissum (SBN 24084387) (Pro Hac Vice)
morgan.grissum@bakerbotts.com
Bryan Parrish (SBN 24089039) (Pro Hac Vice)
bryan.parrish@bakerbotts.com
Casey L. Shomaker (SBN 24110359) (Pro Hac Vice)
casey.shomaker@bakerbotts.com
2001 Ross Avenue, Suite 900
Dallas, TX 75201
Tel: (214) 953-6500
Fax: (214) 953-6503

Wayne O. Stacy (SBN 341579)
wayne.stacy@bakerbotts.com
101 California Street, Suite 3600
San Francisco, CA 94111
Tel: (415) 291-6206
Fax: (415) 291-6306

Attorneys for Plaintiffs
SYMANTEC CORPORATION
and SYMANTEC LIMITED.

BAKER BOTTS L.L.P.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – OAKLAND

SYMANTEC CORPORATION and
SYMANTEC LIMITED,

Plaintiffs,

vs.

ZSCALER, INC,

Defendant.

Case No. 4:17-CV-04414-JST

PLAINTIFFS' SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Judge: Hon. Jon S. Tigar

Plaintiffs Symantec Corporation and Symantec Limited ("Symantec" or "Plaintiffs") file this complaint for patent infringement against Defendant Zscaler, Inc. ("Zscaler" or "Defendant") and in support thereof allege and aver as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq*., specifically including 35 U.S.C. § 271.

THE PARTIES

2. Symantec Corporation is a corporation organized under the laws of the State of Delaware, with a principal place of business at 350 Ellis Street, Mountain View, California.

3. Symantec Limited is a company organized under the laws of the Ireland, with a principal place of business at Ballycoolin Business Park Blanchardstown, Dublin, Co. Dublin 15, Ireland.

4. On information and belief, Zscaler is a corporation organized under the laws of the State of Delaware, with a principal place of business at 110 Rose Orchard Way, San Jose, California.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this patent infringement action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

6. Zscaler is deemed to reside in this judicial district by virtue of being incorporated in the State of Delaware. In addition, on information and belief, Zscaler regularly transacts business in Delaware, including but not necessarily limited to offering products or services that infringe one or more of Symantec's asserted patents to customers located in Delaware and/or for use in Delaware. Accordingly, this Court may properly exercise personal jurisdiction over Zscaler.

7. Venue lies in this judicial district pursuant to 28 U.S.C. §§ 1391(b), 1391(c) and/or 1400(b) at least because Zscaler is deemed to reside in this judicial district by virtue of being incorporated in the State of Delaware. In addition, on information and belief, Zscaler has committed acts of infringement in the State of Delaware, including but not necessarily limited to

offering products or services that infringe one or more of Symantec's asserted patents to customers located in Delaware and/or for use in Delaware.

THE PATENTS-IN-SUIT

8. U.S. Patent No. 8,316,429 ("the '429 Patent"), titled "Methods and Systems for Obtaining URL Filtering Information," was issued by the USPTO on Nov. 20, 2012. Symantec is the owner by assignment of the entire right, title and interest in and to the '429 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '429 Patent is attached hereto as Exhibit D.

9. U.S. Patent No. 8,316,446 ("the '446 Patent"), titled "Methods and Apparatus for Blocking Unwanted Software Downloads," was issued by the USPTO on Nov. 20, 2012. Symantec is the owner by assignment of the entire right, title and interest in and to the '446 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '446 Patent is attached hereto as Exhibit E.

10. U.S. Patent No. 8,402,540 ("the '540 Patent"), titled "Systems and Methods for Processing Data Flows," was issued by the USPTO on March 19, 2013. Symantec is the owner by assignment of the entire right, title, and interest in and to the '540 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '540 Patent is attached hereto as Exhibit F.

11. The'429 Patent, '446 Patent, and '540 Patent are referred to herein collectively as the Patents-in-Suit.

BACKGROUND OF THE DISPUTE

Symantec Is a Pioneer in Fundamental Networking and Security Technology

12. Since its inception, Symantec has been providing software products to enhance its customers' computing productivity, security and reliability. Symantec was founded in 1982 by computer scientist Gary Hendrix with a grant from the National Science Foundation. Originally focused on natural language processing and artificial intelligence-related products, Symantec grew throughout the 1980s through organic growth and strategic acquisitions in the computer software field. In 1990, Symantec merged with Peter Norton Computing, a developer

of various consumer antivirus and data management utilities. At the time, Symantec was already a market leader for Macintosh antivirus and utilities software and had already begun development of a DOS-based antivirus program, making the merger with Norton strategically advantageous. Norton AntiVirus was launched in 1991. In 1993, the Norton product group accounted for 82% of Symantec's total revenues.

13. Among other areas of expansion, Symantec sought to develop and acquire more products for corporate customers. Specifically, Symantec sought to offer products that would serve enterprise environments in which desktop computers were connected with local and other networks. Symantec was determined to achieve a goal of providing integrated, platform independent and centralized network administration solutions. Symantec’s investment and innovation led to the launching the Norton Enterprise Framework in 1996. By the late 1990s, Symantec was marketing three major product lines. The first line covered security and assistance products, consisting mainly of Norton AntiVirus and Norton Utilities products to keep personal computers protected and reliable. The second line included remote productivity solutions, which enabled telecommuters, mobile professionals and workers in remote offices to access information, applications and data on-demand from any location. The third line included internet tools, primarily for Java programmers.

14. On August 1, 2016, Symantec acquired Blue Coat Systems, Inc. (“Blue Coat”). Blue Coat was founded in 1996, and has been a leading provider of advanced web security solutions for global enterprises and governments. Through the acquisition, Symantec expanded and complemented its technology offerings with the addition of Blue Coat’s security platform technology.

15. Symantec (including Blue Coat) has been a market leader with its technology offerings and has been dedicated to continued innovation to help customers secure and manage their information. Symantec expended tremendous resources in research and development to create the intellectual property upon which its products are based. Over the years, Symantec has invested billions of dollars in research and development, and a significant portion of that investment is protected by a portfolio of over 2,000 United States patents.

Zscaler's Infringing Cloud Security Platform

16. Zscaler is a relative newcomer to the network security arena, having been founded in 2008. Zscaler has gained momentum in the marketplace through unlawful use of the technology claimed in the Patents-in-Suit. Symantec is a direct competitor with Zscaler in the network security space, and Zscaler's infringement of the Patents-in-Suit is causing Symantec irreparable harm.

17. On information and belief, Zscaler's cloud security platform, including without limitation its Zscaler Enforcement Node or "ZEN" component (collectively, "the Zscaler Platform"), infringes one or more of the Patents-in-Suit, as described in more detail below.

Zscaler's Infringement is Willful

18. Zscaler has been aware of the Patents-in-Suit and its infringement of those patents since at least the filing of Symantec's Original Complaint in *Symantec Corp. v. Zscaler, Inc.*, Case No. 1:17-cv-00432 (D. Del. Apr. 18, 2017) on April 18, 2017.

19. Symantec's April 18, 2017 Complaint explained how Zscaler met each element of a claim of each of the Patents-in-Suit. Despite this knowledge, Zscaler has deliberately chosen to continue to infringe the Patents-in-Suit by making, using, importing, selling, and/or offering to sell the Zscaler Cloud Security Platform.

20. In addition, on information and belief, the '429 Patent was brought to Zscaler's attention at least through Zscaler's hiring of Lee Dolsen, an inventor of the '429 Patent, from Blue Coat on or around May 28, 2012. On information and belief, Lee Dolsen has a leadership role as a technical director at Zscaler, and has an ownership stake in Zscaler. On information and belief, Zscaler also had knowledge of the '429 Patent through Zscaler's hiring of: (1) Adam Thompson from Blue Coat on or around March 1, 2016; (2) Haggai Polak from Blue Coat on or around December 23, 2015; (3) Mark Ryan from Blue Coat on or around January 8, 2011; and (4) Steve House from Blue Coat on or around September 4, 2015. Nevertheless, Zscaler has continued its infringement of the '429 Patent with full knowledge of that infringement.

21. On information and belief, the '446 Patent was brought to Zscaler's attention at least through Zscaler's hiring of Lee Dolsen, an inventor of the '446 Patent, from Blue Coat on

or around May 28, 2012. On information and belief, Lee Dolsen has a leadership role as a technical director at Zscaler, and has an ownership stake in Zscaler. On information and belief, Zscaler also had knowledge of the ’446 Patent through Zscaler’s hiring of: (1) Adam Thompson from Blue Coat on or around March 1, 2016; (2) Haggai Polak from Blue Coat on or around December 23, 2015; (3) Mark Ryan from Blue Coat on or around January 8, 2011; and (4) Steve House from Blue Coat on or around September 4, 2015. Nevertheless, Zscaler has continued its infringement of the ’446 Patent with full knowledge of that infringement.

22. On information and belief, Zscaler also had knowledge of the ’540 Patent through Zscaler’s hiring of: (1) Adam Thompson from Blue Coat on or around March 1, 2016; (2) Haggai Polak from Blue Coat on or around December 23, 2015; (3) Mark Ryan from Blue Coat on or around January 8, 2011; (4) Steve House from Blue Coat on or around September 4, 2015; and (5) Lee Dolsen from Blue Coat on or around May 28, 2012. Nevertheless, Zscaler has continued its infringement of the ’540 Patent with full knowledge of that infringement.

23. On information and belief, Zscaler’s continued infringement of the Patents-in-Suit has been willful and deliberate. In particular, as set forth below, Zscaler has willfully infringed at least by copying features from Blue Coat’s (now Symantec’s) products that incorporate or reflect the asserted claims of the Patents-in-Suit, failing to conduct a post-filing investigation, failing to take any remedial actions upon learning of the patents, and increasing its acts of infringement since the filing of this case.

24. On information and belief, Zscaler actively recruited and hired away several former employees of Blue Coat in an effort to obtain information about and copy features from Blue Coat’s products. These individuals included, among others, Adam Thompson, Haggai Polak, Lee Dolsen, Mark Ryan, and Steve House.

25. These individuals had knowledge regarding the operation of Blue Coat’s products. For example, Mr. Thompson, Mr. Dolsen, Mr. Ryan, and Mr. House worked on Blue Coat’s ProxySG product before Zscaler hired them away from Blue Coat. While at Blue Coat, Mr. Thompson also worked on Blue Coat’s Malware Analysis, Encrypted Traffic Management, SSL Visibility, Threatpulse, and Packet Shaper solutions. On information and belief, Zscaler

availed itself of Mr. Dolsen's knowledge and assistance to conduct its infringing activities. On information and belief, Zscaler hired Mr. Dolsen, at least in part, to contribute to the development of the technology now accused of infringing at least the '429 and '446 Patents.

26. Zscaler has also demonstrated a deliberate, bad-faith behavior evidencing a pattern of copying of Blue Coat's products. For example, after recruiting Blue Coat employees, those individuals provided information regarding Blue Coat products. Indeed, while at Zscaler, Mr. Ryan provided Zscaler's "tiger team" with what he characterized as a "brain dump" on Blue Coat's Cloud solution.

27. On information and belief, one or more of Mr. Thompson, Mr. Polak, Mr. Dolsen, Mr. Ryan, Mr. House, and other former Blue Coat employees provided Zscaler with information related to Blue Coat's (now Symantec's) claimed technology and products incorporating that technology. On information and belief, Zscaler used that information to copy features from Blue Coat's claimed technology and products incorporating that technology into Zscaler's Cloud Security Platform.

28. On information and belief, Zscaler copied features from Blue Coat's claimed technology and products to compete with Blue Coat and to "steal market share" from Blue Coat. On information and belief, Zscaler has continued to compete with Blue Coat (acquired by Symantec) using the features of the Zscaler Platform copied from Blue Coat's claimed technology and products.

29. Zscaler's deliberate, bad-faith, and flagrant strategy to compete with Blue Coat by copying features from the claimed technology of the Patents-in-Suit constitutes egregious conduct.

30. On information and belief, Zscaler has made no good faith effort to avoid infringement of the Patents-in-Suit. In particular, on information and belief, Zscaler failed to conduct an adequate investigation into Symantec's infringement allegations, thereby evidencing Zscaler's wanton disregard of Symantec's patents. Zscaler's conduct is particularly egregious given that the parties are competitors and Symantec's Complaint requests injunctive relief.

31. On information and belief, Zscaler has taken no remedial actions upon learning of its infringement of the Patents-in-Suit. More specifically, on information and belief, Zscaler has made no attempt to cease its infringing conduct or design around the Patents-in-Suit.

32. Furthermore, Zscaler has increased its infringement of the Patents-in-Suit since the filing of this case. For example, despite knowing of its infringement at least through Symantec's Complaint, Zscaler significantly increased the amount of potentially infringing daily transactions from thirty billion to forty billion. This increase occurred in the July 2017 to December 2017 time period and evidences Zscaler's willful disregard of its infringement of the Patents-in-Suit. As another example, Zscaler's revenue from the sales of the accused features of the Zscaler Platform has continued to increase since the filing of this case.

33. Zscaler's deliberate decision to not only continue but to increase its infringement of the Patent-in-Suit since the filing of this case also constitutes egregious and wanton conduct.

34. In view of the forgoing, Zscaler's infringement of the Patents-in-Suit has been willful, done deliberately and with full knowledge that the use of the Zscaler Cloud Security Platform infringes the Patents-in-Suit, justifying an increase in the damages to be awarded to Symantec up to three times the amount found or assessed, in accordance with 35 U.S.C. § 284.

PATENT INFRINGEMENT CLAIMS

Count I – Infringement of U.S. Patent No. 8,316,429

35. Symantec incorporates by reference the allegations in Paragraphs 1 through 109 above.

36. Prior approaches to network security suffered were deficient when it came to implementing policies to determine which traffic can pass between two networks, such as between a private network and the internet, especially when it comes to secure communications over the Internet. For example, with many Web sites, "the information exchanged between the Internet host(s) and the private network client is passed unencrypted. Hence, the proxy is able to examine the information being passed and evaluate it against its firewall rules to determine whether or not the communications should be allowed." Ex. D, '429 Patent at 1:28-33. But this is not always the case. In some cases, "communications between the private network client and

the Internet host(s) are encrypted so as to prevent eavesdropping by third parties," such as for communications between a client and hosts involved with electronic commerce or banking. *Id.* at 1:34-40.

37. One example of such a secure communication technique is the SSL protocol. SSL is a protocol unique to secure communications over the Internet. It "provides privacy between two communicating applications," such as a client's Web browser and a Web server, by encrypting data exchanged between the client and the server. *Id.* at 4:20-23, 4:31-37. Although encryption offers many benefits (e.g., privacy), it created problems for proxy servers. In particular, one "unfortunate consequence" was that proxy servers were not able to read the messages being passed and therefore had "no way of determining whether their firewall policies are being violated." *Id.* at 1:41-45. As a result, proxy servers were "vulnerable to attacks by computer viruses and other malware," and private network owners/operators were exposed to potential liability due to the possibility of permitting traffic to pass that otherwise would not have been allowed had the proxy been able to apply its policies. *Id.* at 1:45-50. These are problems that specifically arise in computer networks, and in particular in the context of secure communications over the Internet through proxy servers.

38. Prior approaches to providing security in computer networks did not address this unique problem of secure communications over the Internet. A potential solution is to "permit the proxy to decrypt all transmissions between the private network client and the host and subject those decrypted communications to scrutiny according to the firewall policies" as if the original communications had not been encrypted. *Id.* at 1:51-55. Such an approach, however, is unworkable for at least three reasons. First, it defeats the purpose of providing a secure communication mechanism for sensitive data. *See id.* at 1:56-58. Second, the decrypted data at the proxy becomes an attractive target for attacks by third parties that desired to exploit that information. *See id.* at 1:58-60. Third, users are likely to reject such a solution due to the inevitable intrusion into a user's privacy. *See id.* at 1:60-2:3.

39. By January 31, 2006 (the filing date of the application which later issued as the '429 Patent), the inventors had recognized a need for "an effective way to police secure or

encrypted communications between clients and hosts that does not require decryption of the message traffic." *Id.* at 2:4-6. Prior to the invention of the '429 Patent, when encrypted communications such as SSL were used, the URL of the host "could not be extracted from the client's request and, short of decrypting that request, the network administrator" could not prevent undesired access. *Id.* at 6:29-34. To address this unique problem arising in the context of secure communications over the Internet, the inventors of the '429 Patent developed novel and innovative techniques for "extracting and categorizing [URLs] identifying hosts involved in secure Internet communications without having to decrypt [SSL] communications from clients seeking access to such hosts." *Id.* at 1:6-10.

40. The claimed inventions of the '429 Patent solve the problem of being unable to police secure communications over the Internet (a problem specifically arising in the realm of computer networks). Unlike prior approaches, the inventions described and claimed in the '429 Patent "mak[e] use of the characteristics of the SSL handshake," such as "information . . . in the server's digital certificate, to determine whether or not to permit communications between the client and the host." *Id.* at 6:35-39. These methods were and are a significant improvement over (and patentably distinct from) existing approaches. *See* Ex. N, '429 Patent Prosecution History, at 405-417. The approach described and claimed in the '429 Patent overcomes the dilemma posed by secure communications by making use of characteristics of the SSL handshake in a manner that prior approaches could not. *See* Ex. D, '429 Patent at 6:35-39. Specifically, "information contained in the server's digital certificate" is used "to determine whether or not to permit communications between the client and the host." *Id.*

41. As described in the '429 Patent, at the start of an SSL communication, a client transmits a hello message that is received at the proxy/firewall. In response, the proxy/firewall transmits its own hello message to the same IP address that was identified in the client's initial request (i.e., a destination IP address included in the client's hello message, which indicates the entity to which the message is directed). *See id.* at 6:39-52. When the destination server receives the proxy's hello message, it is indistinguishable from any other hello message (i.e., the destination server is unaware that the message is an attempt by the proxy server to determine the

destination server's true identity). *See id.* at 7:10-16. The destination server returns a hello message that includes its certificate.

42. According to an inventive technique of the '429 Patent (and in contrast to prior approaches), when the proxy/firewall receives the destination server's certificate, the proxy/firewall extracts information (such as the host name (typically in the form of a URL), the certificate's issuer, or the signature of the issuer) from the certificate, which can then be used to query a URL database. *Id.* at 7:20-23. Where the host name is used, the proxy then uses category information returned from the URL database to determine whether or not to allow the communication between the client and the destination server and/or whether or not to permit tunneled communications between the two (i.e., allow communications to pass encrypted through the proxy/firewall). *Id.* at 7:20-28. For example, if the host is a trusted entity, SSL communications may be tunneled through the proxy/firewall, ensuring privacy for the client/user. *Id.* at 5:40-43. If not, SSL communications may be decrypted at the proxy/firewall to allow them to be subjected to further scrutiny. *Id.* at 5:43-45.

43. This inventive approach is captured at least in Claims 1 and 13 of the '429 Patent, and their respective dependent claims. The claimed approaches are tied to computers (and in particular, secure communications over the Internet) and cannot be performed by a human alone. For example, Claim 1 recites "extracting, at the proxy, information from the digital certificate associated with the Internet host," "categorizing, at the proxy, said Internet host into one or more content categories according to said information extracted from the digital certificate," and "based on the one or more content categories into which the Internet host is categorized, determining, at the proxy, whether to (i) pass encrypted communication between a client and the Internet host through the proxy without decrypting the encrypted communication at the proxy or (ii) decrypt the encrypted communication between the client and the Internet host so as to permit examination of the encrypted communication at the proxy."

44. According to another inventive aspect of the '429 Patent, "referrer header information" in messages passed between clients and servers is used to determine whether or not to permit downloads of content or other information from an Internet host identified in the

referrer header. *Id.* at 8:4-8. With this technique, the "refer header URL can also be categorized by the proxy/firewall in the manner described above, sometimes permitting access to objects [e.g., images] that otherwise might not be permitted." *Id.* at 8:57-60; *see also id.* at 8:60-9:3. This inventive approach is captured in independent Claim 10, in which a proxy categorizes the referring source of a request for an object into one or more content categories and determines, based on the one or more content categories into which the referring source is categorized, whether communications should be passed between the client and an Internet host without decryption. The claimed approach is tied to computers (and in particular, secure communications over the Internet) and cannot be performed by a human alone.

45. These claim elements, individually or in combination, are unconventional and nothing in the specification describes these concepts as well-understood, routine, or conventional. To the contrary, the specification describes that with prior approaches "the URL of the host . . . could not be extracted from the client's request and, short of decrypting that request, the network administrator may be unable to prevent the undesired access." *Id.* at 6:29-34. Prior approaches therefore lacked "an effective way to police secure or encrypted communications between clients and hosts that does not require decryption of the message traffic." *Id.* at 2:4-6. Thus, for example, the steps of "extracting, at the proxy, information from the digital certificate associated with the Internet host," "categorizing, at the proxy, said Internet host into one or more content categories according to said information extracted from the digital certificate," and "based on the one or more content categories into which the Internet host is categorized, determining, at the proxy, whether to (i) pass encrypted communication between a client and the Internet host through the proxy without decrypting the encrypted communication at the proxy or (ii) decrypt the encrypted communication between the client and the Internet so as to permit examination of the encrypted communication at the proxy" capture an unconventional approach to policing secure communications that was unknown in the field before the invention of the '429 Patent. These claimed concepts solve the problems described above and provide the advantages and improvements to computers described below.

46. Notably, the claimed inventions of the ’429 Patent do not foreclose alternative approaches to policing secure communications. That the claimed inventions of the ’429 Patent do not foreclose alternative approaches to managing bandwidth is evidenced by the substantial number of patents that have issued after the disclosure of the ’429 Patent had been considered during prosecution of those patents. For example, on information and belief at least 6 U.S. Patents have issued after the disclosure of the ’429 Patent was considered during prosecution. *See* Ex. U. Thus, rather than preclude all approaches to policing secure communications, the claimed inventions of the ’429 Patent are novel techniques that offered significant technical advantages over alternative approaches, as described in more detail below.

47. The inventions described and claimed in the ’429 Patent improve the functioning of the computer systems in which they are implemented. For example, prior to the invention of the ’429 Patent, proxy servers and other network entities were unable to effectively police secure or encrypted communications between clients and hosts without decrypting all message traffic. *Id.* at 2:4-6. Decrypting all transmissions, however, made the proxy an attractive target for attacks by third parties seeking to exploit that information and defeated the purpose of providing secure communications in the first instance. The inventions described and claimed in the ’429 Patent solved these problems and thereby improved the functioning of the proxy servers in which they were implemented by providing an effective means of policing secure communications without decrypting all traffic.

48. In addition to improving the functionality of existing proxy servers, the claimed inventions of the ’429 Patent offered a number of additional technical advantages over prior approaches. As one example, the claimed invention of the ’429 Patent allowed “network managers to leverage URL databases used for categorizing servers or other Internet hosts for use even with SSL communication sessions,” something that had not been achieved with prior approaches. *Id.* at 5:45-48.

49. As another example, the claimed inventions of the ’429 Patent enables a proxy to use the URL of the certificate’s issuer to make policy decisions, which advantageously allowed the proxy to determine whether the issuer is a recognized and/or trusted issuer. *Id.* at 7:52-58.

This is advantageous in that it may "help prevent fraud, for example, where a host provider has attempted to counterfeit a certificate." *Id.* at 7:58-59. As still another example, the claimed inventions of the '429 Patent advantageously enables the proxy to "verify the signature of the issuer as attached to the certificate" in order to confirm the legitimacy of the destination server. *Id.* at 7:59-66.

50. As yet another example, the claimed inventions of the '429 Patent advantageously enables a proxy server to make use of referrer header categorization to permit/deny communications between clients and servers, which can improve the granularity of the URL filtering, "sometime permitting access to objects that otherwise might not be permitted." *Id.* at 8:57-60.

51. The approaches described and claimed in the '429 Patent represented a significant advance over the prior approaches that were not well-known, routine, or conventional in the field at the time the '429 Patent was filed. On information and belief, during examination of the application which ultimately issued as the '429 Patent, the patent examiner at the USPTO considered at least 24 U.S. patent documents, as well as one other publication. *See id.* at Cover Page. *See also* Ex. N, '429 Patent Prosecution History, at 68, 70-80, 117-127, 161-175, 177, 205-206, 208-224, 250, 252-269, 303, 305-325, 363-365, 367-385, 418-421, 423-461 (describing search results and references considered). These include references from IBM, Microsoft Corporation, prior Symantec and Blue Coat solutions, amongst others. The patent examiner determined that none disclosed or rendered obvious the inventions of the '429 Patent. *See* Ex. N, '429 Patent Prosecution History, at 405-417 (notice of allowance). Indeed, the examiner stated that "[n]one of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed." *Id.* at 415.

52. On information and belief, Zscaler directly infringes one or more claims of the '429 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

53. Claim 1 of the ’429 Patent recites as follows:

> A method, comprising:
>
> receiving, at a proxy, a client hello message from a client;
>
> transmitting, from said proxy to an Internet host, a request for a digital certificate associated with the Internet host;
>
> extracting, at the proxy, information from the digital certificate associated with the Internet host;
>
> categorizing, at the proxy, said Internet host into one or more content categories according to said information extracted from the digital certificate, said categorizing including maintaining a table at said proxy wherein each Internet host is associated with a category which defines attributes of the Internet host or content associated with the Internet host; and
>
> based on the one or more content categories into which the Internet host is categorized, determining, at the proxy, whether to (i) pass encrypted communication between a client and the Internet host through the proxy without decrypting the encrypted communication at the proxy or (ii) decrypt the encrypted communication between the client and the Internet host so as to permit examination of the encrypted communication at the proxy.

54. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of Claim 1. Zscaler’s cloud security platform, including its ZEN component, receive, at a proxy (e.g., a ZEN), a client hello message from a client. For example, Zscaler’s ZEN component receives a client hello message from a client (e.g., a subscriber’s computer) in the form of an HTTPS request from the client. Zscaler’s cloud security platform, including its ZEN component, transmit, from the proxy to an Internet host, a request for a digital certificate associated with the Internet host. For example, Zscaler’s ZEN component transmits an HTTPS request to a destination server thereby initiating an SSL handshake. Zscaler’s cloud security platform, including its ZEN component, extracts information from the digital certificate associated with the Internet host. For example, Zscaler’s ZEN component receives a certificate from the destination server and reads information from the certificate during validation of the destination server. Zscaler’s cloud security platform, including its ZEN component, categorizes the Internet host into one or more content categories according to the information extracted from

the digital certificate. For example, Zscaler's ZEN component categorizes URLs into various different classes, supercategories, and categories consistent with information extracted from the destination server's certificate. Zscaler's cloud security platform, including its ZEN component, maintains a table at the proxy wherein each Internet host is associated with a category that defines attributes of the Internet host or content associated with the Internet host. For example, Zscaler's cloud security platform includes a table for each class, supercategory, and category that associates URLs with particular categories. The categories further include attributes that define the Internet host or content associated with the host, such as a description of the "gambling" category that defines attributes of "gambling" sites as "sites that provide online gambling or are related to gambling assistance, training, information, or advocacy." Zscaler's cloud security platform, including its ZEN component, based on the one or more content categories into which the Internet host is categorized, determines whether to (i) pass encrypted communication between a client and the Internet host through the proxy without decrypting the encrypted communication at the proxy or (ii) decrypt the encrypted communication between the client and the Internet host so as to permit examination of the encrypted communication at the proxy. For example, Zscaler's cloud security platform permits SSL configuration such that SSL communications that fall within certain URL categories are passed from the destination server to the client through the ZEN without decrypting the communication. If the SSL communication does not fall within one of the specified URL categories, then the communication is decrypted so that the ZEN can inspect the decrypted communication for, among other things, data leakage, malicious content, viruses, and to enforce policy. As such, the ZEN determines whether to pass the encrypted SSL communication or decrypt the communication based on the categorization of URLs into content categories.

55. In view of the foregoing, Zscaler directly infringes the '429 Patent in violation of 35 U.S.C. § 271(a).

56. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '429 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '429 Patent, Zscaler is inducing

infringement of the ’429 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler’s marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the ’429 Patent.

57. Symantec has no adequate remedy at law for Zscaler’s acts of infringement. As a direct and proximate result of Zscaler’s acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler’s acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

Count II – Infringement of U.S. Patent No. 8,316,446

58. Symantec incorporates by reference the allegations in Paragraphs 1 through 132 above.

59. There are dangers and risks associated with connecting a computer to the Internet, such as computer viruses that spread from computer to computer (for example, using e-mail). Ex. E, ’446 Patent at 1:20-24. There were also other types of unwanted software that could be harmful to the operation of a computer. Spyware and Trojans are two examples of these kinds of threats to computer and data safety. *Id.* at 1:24-25. “Spyware is malicious code that covertly monitors actions taken on a PC, and reports those activities to an outside entity. For example, spyware can log and report all websites visited by a user, along with other personal data such as passwords, bank accounts, social security numbers, and so on.” *Id.* at 1:25-30. Trojans, meanwhile, “are programs that appear legitimate, but perform some illicit activity when executed,” such as locating password information, making a system more vulnerable to subsequent attacks, or destroying programs or data stored on the computer. *Id.* at 1:31-35. Problematically, Trojans often sneak into computer systems disguised in free games or other utilities, and remain in the computer doing damage or permit a third party to take control of the computer. *Id.* at 1:35-40. These are problems that specifically arise in computer networks.

60. Prior approaches to network security were not able to provide adequate protection against these unwanted software downloads. Unwanted software is “often sent as executable files—such as those having .EXE (executable), .COM (command), or .DLL (dynamic linked library) file extensions—or active content files—such as those having .CAB (cabinet) and .OCX

(OLE control extension) file extensions. Spyware, however, "may be disguised in some fashion to pass through" a URL scanner, such as "file extensions camouflaged to disguise their true nature." *Id.* at 5:1-6. Likewise, Trojans "often sneak in attached to a free game or other utility." *Id.* at 1:37-38. These features of unwanted software like spyware and Trojans made it difficult for prior network security elements to provide adequate protection against these threats.

61. By April 22, 2005 (the date on which the application which subsequently issued as the '446 Patent was filed), the inventors of the '446 Patent (employees of Blue Coat) recognized the need for a "comprehensive system to block unwanted software downloads and installations." *Id.* at 1:41-42. In particular, the inventors developed new methods and apparatus to block unwanted software downloads, for example at gateway to enterprise or home networks. These methods and systems were and are a significant improvement over (and patentably distinct from) existing approaches to network security, which failed to provide comprehensive protection against unwanted software downloads. *See* Ex. O, '446 Patent Prosecution History, at 23-34.

62. Specifically, the claimed inventions of the '446 Patent provide protection against unwanted software downloads by enabling network devices (such as a proxy server or a firewall) to block unwanted software downloads from Web sites. As described and claimed in the '446 Patent, a proxy server may use a URL filter to categorize a URL from which a download is arriving at the system. Ex. E, '446 Patent at 6:65-7:3. The proxy server can employ a URL database to categorize the URL that originated a download by matching the source URL against the URL database and retrieving the category associated with the source URL. *Id.* at 7:27-30. For example, a URL may be categorized as a "gaming" site. In some instances, a URL may be categorized on a "blacklist" that may indicate downloads from that URL should be blocked or on a "whitelist" that may indicate downloads from that URL should be allowed.

63. In other cases, however, a URL may not be categorized into either a "blacklist" or a "whitelist" and thus more information may be required to determine whether to block a software download from such a URL. To address this problem, the claimed inventions of the '446 Patent provide for blocking or not blocking an attempted download based on a

categorization of the URL from which the download is attempted, the file type of the software being downloaded, and whether downloads of that particular file type are permitted for that category of Web sites. The claimed methods and systems employ a file type identifier "configured to identify the download by file type." *Id.* at 7:38-40. The file type identifier can identify the file type using a file type database that can include a file type extension list associating file types with file extensions and/or a file type signature list that includes signatures of various file types and the file types with which they are associated. *Id.* at 7:52-54, 7:62-65.

64. The use of the file type signatures list is especially advantageous in handling files, such as spyware, that have file extensions camouflaged to disguise their true nature. For example, "to prevent downloads of files that may have file extensions camouflaged to disguise their true nature," the proxy server is "configured to scan incoming files for spyware signatures that cannot be hidden (e.g., through changes in file extensions) and take action according to user-defined spyware policies." *Id.* at 5:1-9. The claimed invention of the '446 Patent leverages the fact that spyware, by its nature, contains certain patterns that the spyware scanner can read in order to identify the true nature of the associated file. *Id.* at 5:10-13. As one example, "a .CAB file will include a header having a certain format," and the file signature list may include information about known characteristics of spyware headers and the like. *Id.* at 5:12-19. The file type identifier can scan the file being downloaded, compare the scanned information with the signature information, and determine the file type based on the signature (even if the file extension has been changed to mask the true nature of the file). *Id.* at 5:19-24, 7:65-8:3.

65. The proxy server can then block or allow the software download based on the categorization and the file type. This information can be used in a variety of ways, advantageously providing operators a more flexible and nuanced approach to protecting against unwanted software downloads. For example, "the blocking decision module can implement a blocking rule to block all .CAB files from URLs on the URL blacklist," whether "the .CAB file was identified by file extension or by signature." *Id.* at 8:11-14. "Another blocking rule can block all downloads from non-whitelisted URLs where the file type identified by file extension does not match the file type identified using the signature list." *Id.* at 8:14-17. As another

example using the "gaming" sites category discussed above, the blocking decision module "can be configured to allow executable (.EXE) files to be downloaded from known gaming sites, but not cabinet (.CAB) files. Since most online games require downloading some executable code, a .EXE download does not look very suspicious from a site in this category. However, a .CAB file from a gaming site would highly likely contain unwanted code." *Id.* at 8:18-25.

66. This inventive approach is captured in at least in Claims 1, 5, and 8, and their respective dependent claims. The claimed approaches are tied to computers and cannot be performed by a human alone. For example, Claim 1 recites "intercepting at a Uniform Resource Locator (URL) filter module of a network device, an attempted download of a file from a URL," "categorizing by the URL filter module of the network device the URL into a URL category according to a URL database," "analyzing by a file type identifier module of the network device the file to determine its file type . . . by detecting one or more of a file type signature in the file and a file extension of the file," "identifying the file type based on one or more of the file type signature detected in the file and the file extension of the file," and "blocking or not blocking the attempted download according to a decision output of a blocking decision module of the network device which receives as inputs the URL category and the file type." If the URL category does not indicate a blacklist or a whitelist, "the URL category specifies a URL content category indicating a type of content provided by the URL and the decision output is based on whether files of said file type are permitted for URLs in the URL content category."

67. These claim elements, individually or in combination, are unconventional, and nothing in the specification describes these concepts as well-understood, routine, or conventional. To the contrary, the specification describes that prior approaches to network security were not able to provide adequate protection against unwanted software downloads, and in particular those that "may be disguised in some fashion to pass through" a URL scanner, such as "file extensions camouflaged to disguise their true nature." *See id.* at 5:1-6. These features of unwanted software like spyware and Trojans made it difficult for prior network security elements to provide adequate protection against these threats. Thus, for example, the steps of "intercepting at . . . a network device, an attempted download of a file from a URL,"

"categorizing . . . the URL into a URL category according to a URL database," "analyzing . . . the file to determine its file type . . . by detecting one or more of a file type signature in the file and a file extension of the file," "identifying the file type based on one or more of the file type signature detected in the file and the file extension of the file," and "blocking or not blocking the attempted download according to a decision output of a blocking decision module of the network device which receives as inputs the URL category and the file type" capture an unconventional approach to blocking unwanted software downloads that was unknown in the field before the invention of the '446 Patent. The functions of the claimed URL filter module, file type identifier module, and blocking decision module recited in the claims, in combination, perform unconventional functions that were not performed in prior systems or methods. Indeed, these claimed concepts solve the problems described above and provide the advantages and improvements to computers described below.

68. Notably, the claimed inventions of the '446 Patent do not foreclose alternative approaches to blocking unwanted software downloads. That the claimed inventions of the '446 Patent do not foreclose alternative approaches to blocking unwanted software downloads is evidenced by the substantial number of patents that have issued after the disclosure of the '446 Patent had been considered during prosecution of those patents. For example, on information and belief at least 9 U.S. Patents have issued after the disclosure of the '446 Patent was considered during prosecution. *See* Ex. V. Thus, rather than preclude all approaches to blocking unwanted software downloads, the claimed inventions of the '446 Patent are novel techniques that offered significant technical advantages over alternative approaches, as described in more detail below.

69. The inventions described and claimed in the '446 Patent improve the functioning of the computer networks in which they are implemented. For example, prior to the invention of the '446 Patent, the performance of computer systems often suffered due to a failure to block unwanted software downloads (such as computer viruses, worms, spyware, and Trojans), leading to system instability, malfunction, and/or loss of critical files. For example, the damage caused by undetected viruses can range from mildly annoying effects to damage to hardware,

software, or files. As another example, a worm introduced into a computer system can consume too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. As another example, computer systems that have been compromised by a Trojan horse may allow malicious users and/or programs access to the computer system to steal confidential and personal information. The inventions described and claimed in the ’446 Patent solved these problems by providing a comprehensive system to block unwanted software downloads and installations, thereby reducing or eliminating the above-described consequences that can result from unwanted software downloads.

70. Moreover, the inventions described and claimed in the ’446 Patent offered a number of additional technical advantages over prior approaches. Unlike prior approaches, the claimed invention of the ’446 Patent enables URL category and file type of an attempted download to be taken into account in blocking attempted downloads. This advantageously allows for the implementation of a variety of blocking rules, and permits a more comprehensive approach to protecting against software downloads while permitting flexibility in the rules that are applied to various URLs. The functioning of the systems (e.g., proxy server or firewall) in which the methods are employed are thereby improved. As another example, the claimed invention of the ’446 Patent provides an effective mechanism for combatting spyware that may be disguised in some fashion to evade existing network security solutions (e.g., spyware having camouflaged file extensions). Furthermore, the ’446 Patent improves existing systems by allowing them to recognize situations in which the file type extension of an attempted download does not match the file type signature and block or allow the download based on rules tailored to that particular circumstance.

71. The approaches described and claimed in the ’446 Patent represented significant advances over prior approaches that were not well-known, routine, or conventional. On information and belief, during examination of the application which ultimately issued as the ’446 Patent, the patent examiner at the USPTO considered at least 33 U.S. patent documents, as well as 4 other publications. *See id.* at Cover Page. *See also* Ex. O, ’446 Patent Prosecution History, at 36-42, 45-69, 127-145, 176, 179-197, 231, 234-249, 288-299, 302-303, 318-324,

356, 359-370, 392, 394-404, 441, 443-447, 485, 487-491 (describing search results and references considered). These include references describing solutions from Microsoft Corporation and IBM, amongst others. The patent examiner determined that none disclosed or rendered obvious the inventions of the ’446 Patent. *See* Ex. O, ’446 Patent Prosecution History, at 23-34 (notice of allowance). Indeed, the examiner stated that the “prior art of record does not explicitly teach or fairly suggest, either individually or in combination, file type and file extension of the files are two entities and blocking or not blocking the attempted download according to a decision output of a blocking decision module of the network device which receives as inputs the URL category and the file type, wherein (i) if the URL category indicates a blacklist, the decision output is to block the download, (ii) if the URL category indicates a whitelist, the decision output is to allow the download, otherwise, the URL category specifies a URL content category indicating a type of content provided by the URL, and the decision output is based on whether files of said file type are permitted for URLs in the URL content category,” as described and claimed in the ’446 Patent. *Id.* at 33.

72. On information and belief, Zscaler directly infringes one or more claims of the ’446 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

73. Claim 1 of the ’446 Patent recites as follows:

> A method, comprising:
>
> intercepting at a Uniform Resource Locator (URL) filter module of a network device, an attempted download of a file from a URL;
>
> categorizing by the URL filter module of the network device the URL into a URL category according to a URL database;
>
> analyzing by a file type identifier module of the network device the file to determine its file type, wherein the file type of the file is determined by detecting one or more of a file type signature in the file and a file extension of the file, and identifying the file type of the file based on one or more of the file type signature detected in the file and the file extension of the file; and
>
> blocking or not blocking the attempted download according to a decision output of a blocking decision module of the network device which receives as

> inputs the URL category and the file type, wherein (i) if the URL category indicates a blacklist, the decision output is to block the download, (ii) if the URL category indicates a whitelist, the decision output is to allow the download, otherwise, the URL category specifies a URL content category indicating a type of content provided by the URL, and the decision output is based on whether files of said file type are permitted for URLs in the URL content category.

74. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of Claim 1. Zscaler's cloud security platform, including its ZEN component, intercepts at a Uniform Resource Locator (URL) filter module of a network device, an attempted download of a file from a URL. For example, Zscaler's ZEN component inspects files being returned from an Internet host (e.g., www.google.com) to a client. Zscaler's cloud security platform, including its ZEN component, categorizes by the URL filter module of the network device the URL into a URL category according to a URL database. For example, Zscaler's ZEN categorizes URLs into URL categories (e.g., the classes, supercategories, or categories used in URL filtering) according to a URL database (e.g., the global URL category database). Zscaler's cloud security platform, including its ZEN component and its File Type Analysis module, analyzes by a file type identifier module of the network device the file to determine its file type, wherein the file type of the file is determined by detecting one or more of a file type signature in the file and a file extension of the file. For example, Zscaler's ZEN component analyzes files, such as attachments to e-mails or HTTP transactions, to detect the file type (e.g., executable, Office document, archive file, image, audio, video, etc.) by scanning the files to determine the file extension (e.g., .exe, .scr, etc.). Zscaler's cloud security platform, including its ZEN component, identifies the file type of the file based on one or more of the file type signature detected in the file and the file extension of the file. As discussed above, for example, Zscaler's ZEN identifies file type by scanning a file to determine the file's extension. Zscaler's cloud security platform, including its ZEN component, blocks or does not block the attempted download according to a decision output of a blocking decision module of the network device which receives as inputs the URL category and the file type. As noted above, for example, the Zscaler's ZEN knows a URL category and a file type. The ZEN will output a decision that either blocks or does not block an attempted download. If the ZEN's File Type Policy specifies a URL category as a blacklist, the ZEN's decision is to

block the download. For example, the ZEN may block particular types of files within the webmail URL category if the URL is blacklisted. Alternatively, the ZEN's File Type Policy may indicate that the URL category is whitelisted and not block the download. Otherwise, the URL category specifies a URL content category indicating a type of content provided by the URL, and the decision output is based on whether files of said file type are permitted for URLs in the URL content category. Zscaler utilizes URL content categories in the form of classes, supercategories, and categories. For example, Zscaler utilizes a class of legal liability, a supercategory of adult material, and a category of adult themes. If the File Type Policy does not specify that the file type is allowed or blocked for a particular URL category, the ZEN determines if files of the particular file type are permitted for URLs in the particular URL content category. For example, if no File Type Policy is specified for executable files downloaded from adult themed websites, the ZEN determines whether to block or allow the download based on whether downloading executable files is permitted for URLs within the adult themed URL content category.

75. In view of the foregoing, Zscaler directly infringes the ’446 Patent in violation of 35 U.S.C. § 271(a).

76. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the ’446 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the ’446 Patent, Zscaler is inducing infringement of the ’446 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the ’446 Patent.

77. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

78. Zscaler without authority supplied or caused to be supplied in or from the United States all or a substantial portion of the components of the invention of the ’446 Patent, where

such components are uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the patents if such combination occurred within the United States. For example, Zscaler's Cloud Security Platform relies upon world-wide data centers. *See, e.g.*, Zscaler, Cloud Architecture Security as a Service, available at https://www.zscaler.com/products/cloud-architecture-security-as-a-service. Zscaler uses servers to enforce security policies in each of the world-wide data centers. *Id.* Zscaler has supplied servers from the United States and installed those servers in foreign data centers. *See, e.g.*, Zscaler, Cloud Enforcement Node Ranges, available at https://ips.zscaler.net/cenr. Zscaler separately transmits its compiled source code from the United States to the servers at data centers outside of the United States. Zscaler actively induces the combination of the servers and the compiled source code at foreign data centers. Zscaler, without permission from Symantec, supplied and/or caused to be supplied in or from the United States all or a substantial portion of the hardware and/or software components of the Zscaler platform (e.g., servers and/or compiled source code), which infringes the '446 Patent, where such components were uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States (e.g., at Zscaler foreign data centers) in a manner that would infringe the patents if such combination occurred within the United States. In view of the foregoing, the Zscaler Platform infringes the '446 Patent in violation of 35 U.S.C. § 271(f)(1).

79. Zscaler without authority supplied or caused to be supplied in or from the United States at least one component of the '446 patented invention that is especially made or especially adapted for use in the '446 patented invention and not a staple article or commodity of commerce suitable for substantial noninfringing use, where such component is uncombined in whole or in part, knowing that such component is so made or adapted and intending that such component will be combined outside of the United States in a manner that would infringe the patent if such combination occurred within the United States. For example, Zscaler's Cloud Security Platform relies upon world-wide data centers. Zscaler, Cloud Architecture Security as a Service, available at https://www.zscaler.com/products/cloud-architecture-security-as-a-service.

Zscaler uses servers to enforce security policies in each of the world-wide data centers. *Id.* Zscaler has supplied servers from the United States and installed those servers in foreign data centers. *See, e.g.*, Zscaler, Cloud Enforcement Node Ranges, available at https://ips.zscaler.net/cenr. Zscaler separately transmits its compiled source code from within the United States to the servers in data centers outside of the United States intending to combine the source code with servers in the foreign data centers. Zscaler, without permission from Symantec, supplied and/or caused to be supplied in or from the United States hardware and/or software components (e.g., servers and/or compiled source code) of the Zscaler Platform that—as Zscaler knows—are especially made or especially adapted for use in the '446 patented invention and are not a staple article or commodity of commerce suitable for substantial non-infringing use, where such components were uncombined in whole or in part, intending that the hardware and/or software components of the Zscaler Cloud Security Platform will be combined outside of the United States (e.g., at Zscaler foreign data centers) in a manner that would infringe the patents if such combination occurred within the United States. In view of the foregoing, the Zscaler Platform infringes the '446 Patent in violation of 35 U.S.C. § 271(f)(2).

Count III – Infringement of U.S. Patent No. 8,402,540

80. Symantec incorporates by reference the allegations in Paragraphs 1 through 152 above.

81. The '540 Patent is generally directed to improved computer, network, and web security. *See* Ex. F, '540 Patent at Col. 1:66 – 2:3; *see also id.* at 3:14-20.

82. The inventors of the '540 Patent identified a growing technological problem with the way Web and network security was being implemented in the early-to-mid 2000s. At the time of the filing of the '540 Patent, existing web security systems suffered from technical shortcomings based on those systems' failures to address the evolving use of the Internet and growing prominence of a mobile workforce (i.e., "remote site connectivity"). *See id.* at 2:52-55. The prior approaches of dealing with the "disparate threats" facing a network (e.g., "viruses, attacks by hackers, spyware, phishing, spam, intrusion onto a computer network by unauthorized users, and others"), such as providing a number of different products "that separately

address[ed] each of the most prevalent type of threats" or "monolithic networking hardware" systems that "joined together" products that "address each of the most prevalent type of threats," were still "hardwired to provide a set of services." *Id.* at 2:5-18, 2:33-37.

83. The inventors of the '540 Patent had the foresight to understand how the Internet's influence in the business landscape would affect web security. By the early 2000s, companies were depending "upon the Internet for additional business-critical activities like supply chain integration, long-distance communications, and remote site connectivity." *Id.* at 2:52-55. However, "each Internet-based endeavor potentially open[ed] another door to outside hackers and malicious code attacks." *Id.* at 2:55-57. External web access to information on a network, however, was critical to the efficient and effective workings of enterprises." *Id.* at 4:25-26. "Employees, partners, customers, and remote users need timely access using a wide variety of communication methods and devices from all locations. Additionally, the confidentially [sic] and integrity of network resources such as intellectual property, competitively advantaged data, regulated or personal data must be maintained in this open environment. However, threats of attack, intrusion, and espionage may come in a wide variety of forms such as spyware, keystroke loggers, and Trojans, while malware such as worms and viruses must also be detected and prevented." *Id.* at 4:26-36. The '540 Patent recognized that "[n]etwork security management involves balancing a complex array of network participant needs," and that "[p]roviding a network security solution that effectively delivers all of one participant's access needs may impose constraints on one or many other participants' needs such as making critical aspects of the network vulnerable to intrusions." *Id.* at 4:37-51.

84. A potential solution is to physically segment the network using multiple network management devices. However, "[s]ince all, or nearly all of the data accessed and used by internal users, external users, clients, servers, vendors, and the like passes through an organization's network, segmenting the network to address the various needs of the network participants can be costly because of the substantial expense associated with hardware security facilities." *Id.* at 4:52-57. Moreover, "segmenting may not relieve the constraints sufficiently to justify this expense" and "management of segmented, network management devices increases

complexity which may create new opportunities for segments being vulnerable to intrusion." *Id.* at 4:57-62. Thus, physically segmenting network participants is "neither practical nor in most cases possible while still delivering effective business solutions throughout the network." *Id.* at 4:63-65. These are problems that specifically arise in computer networks.

85. Accordingly, the inventors of the '540 Patent understood the technical need for "more effective unified threat management techniques" (*Id.* at 3:6-10) while providing a web security solution that was adapted to protect expanding networks and user productivity. *Id.* at 3:6-10. *See also id.* at 2:50-52 ("Companies' computing systems are more interconnected than ever, with the promise that network expansion will only continue."); 2:61-63 ("[C]ompanies must grapple with how to keep their network safe, without sacrificing growth or productivity."). The inventors of the '540 Patent recognized that "[a]n approach to allow managed separation of aspects of a network security system based on participant criteria may include virtualization of the network." *Id.* at 4:67-5:2. As described in the '540 Patent, network virtualization advantageously allows one or more participants (or participant types) to be "logically connected to the network through a virtual network connection within a network security system," such as a flow processing system implemented at a proxy server. *Id.* at 5:2-6; 21:3-24.

86. The inventors of the '540 Patent developed a virtualized network security system (VNSS) that provides security policies to data flows received at the VNSS, as well as methods for securing a plurality of virtual networks with a VNSS and configuring virtual network security in a VNSS. These systems and methods were and are a significant improvement over (and patentably distinct from) prior approaches to network security. *See* Ex. P, '540 Patent Prosecution History, at 1148-1156 (notice of allowance). The '540 Patent explains that the VNSS may provide security policies "regardless of the physical arrangement of the network." Ex. F, '540 Patent at 85:42-45. For example, users may connect to the VNSS using the Internet, a VPN, or other wireless connection. *See id.* at 85:57-62. The virtualization may be applied "to provide a logical arrangement of policies, networks, behavioral analyses, applications" and combinations thereof to enable the flow processing facility to "provides its features and functions in ways that are logically beneficial or convenient; logically tailored to data flows or to

users of data flows; [and] consistent with an abstract and logical model (as opposed to a literal and physical model)." *Id.* at 21:49-57.

87. Unlike existing approaches, the virtualized nature of the '540 Patent's security system allows the VNSS to provide a logical arrangement of security policies without having to physically separate the data flow as was required by prior art systems relying on multiple disparate components to provide security. *See id.* at 21:49-52. For example, virtualization may present a server computing facility with "different policies, networks, behavioral analyses, applications, and so on than it provides to a network-connected computing facility." *Id.* at 21:57-61. The '540 Patent explains that the flow processor may identify a specific data flow coming from a participant and "logically route" the flow "to a virtual network [] associated with that participant" at which point a specific security policy may be applied to the virtual network. *Id.* at 86:26-35.

88. For example, two servers may each communicate with a database over the network. If the network were physically segmented, "such as with a network security appliance physically residing between the servers and the database, both servers may be subjected to one intrusion detection and prevention policy." *Id.* at 85:37-42. However, using the "virtualized network security system" described and claimed in the '540 Patent, multiple virtual networks connected to the database can be supported, regardless of the physical arrangement of the network. *Id.* at 85:42-45. Advantageously, "each of the servers in this example may be connected to the database through different virtual networks," and "[t]he security policy on each of the virtual networks may be different and, perhaps, a function of the server's identity." *Id.* at 85:45-49.

89. This inventive approach is captured in at least in Claims 1, 6, and 13 of the '540 Patent, and their respective dependent claims. The claimed approaches are tied to computers and cannot be performed by a human alone. For example, Claim 13 recites "[a] virtualized network security system (VNSS)" comprising "a plurality of flow processing facilities configured as elements of the VNSS for processing a data flow . . . comprising subscriber profile data," "a first security policy for a first virtual network," "a second security policy for a second

virtual network," in which "the plurality of flow processing facilities make a first determination, in accordance with one of the first security policy and the second security policy, of abnormalities that are associated with the data flow, the first determination based at least in part on the subscriber identified by the subscriber profile data" and "the plurality of flow processing facilities make a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data."

90. These claim elements, individually or in combination, are unconventional, and nothing in the specification describes these concepts as well-understood, routine, or conventional. To the contrary, the specification describes that prior approaches to network security failed to provide "a network security solution that effectively delivers all of one participant's access needs" without imposing "constraints on one or many other participants' needs." *See id.* at 4:47-57. Potential approaches such as physically segmenting the network were "costly because of the substantial expense associated with hardware security facilities" (*Id.* at 4:52-57), did "not relieve the constraints sufficiently to justify this expense," and increased management complexity in a manner that created opportunities for segments being vulnerable to intrusion. *Id.* at 4:57-62. Thus, for example, the elements of a "[a] virtualized network security system (VNSS)" comprising "a plurality of flow processing facilities configured as elements of the VNSS for processing a data flow . . . comprising subscriber profile data," "a first security policy for a first virtual network," "a second security policy for a second virtual network," in which "the plurality of flow processing facilities make a first determination, in accordance with one of the first security policy and the second security policy, of abnormalities that are associated with the data flow, the first determination based at least in part on the subscriber identified by the subscriber profile data" and "the plurality of flow processing facilities make a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data" captured an unconventional approach to network security that was unknown in the field before the

invention of the ’540 Patent. These claimed concepts solve the problems described above and provide the advantages and improvements to computers described below.

91. Notably, the claimed inventions of the ’540 Patent do not foreclose alternative approaches to network security. That the claimed inventions of the ’540 Patent do not foreclose alternative approaches to network security is evidenced by the substantial number of patents that have issued after the disclosure of the ’540 Patent had been considered during prosecution of those patents. For example, on information and belief at least 155 U.S. Patents have issued after the disclosure of the ’540 Patent was considered during prosecution. *See* Ex. W. Thus, rather than preclude all approaches to network security, the claimed inventions of the ’540 Patent are novel techniques that offered significant technical advantages over alternative approaches, as described in more detail below.

92. The inventions described and claimed in the ’540 Patent improve the functioning of the computer networks in which they are implemented. For example, prior to the invention of the ’540 Patent, network security systems could not effectively meet all of one participant’s access needs without imposing constraints on one or many other participants’ needs such as making critical aspects of the network vulnerable to intrusions. *See id.* at 4:47-51. The inventions described and claimed in the ’540 Patent solved these problems and thereby improved the functioning of the networks in which they were implemented by enabling “managed separation of aspects of a network security system based on participant criteria” through virtualization of the network. *Id.* at 4:67-5:2. The network virtualization achieved by the solutions claimed in the ’540 Patent allowed “one or more participants (or participant types) to be logically connected to the network through a virtual network connection within a network security system such as the flow processing facility.” *Id.* at 5:2-6. Unlike prior approaches, the virtualized network security system described and claimed in the ’540 Patent can be applied “to provide a logical arrangement of policies, networks, behavioral analyses, applications, any and all combinations of the foregoing, and so on” and enable the flow processing facility “to provide its features and functions in ways that are logically beneficial or convenient; logically tailored to data flows or to users of data flows; consistent with an abstract and logical model (as opposed to

a literal and physical model); and so forth." *Id.* at 21:49-57. Thus, unlike physically segmenting the network, the claimed virtualized network security system permits different policies, networks, behavioral analyses, applications, and so on to be applied to different servers or network-connected computing facilities. *See id.* at 21:57-61.

93. The inventions described and claimed in the ’540 Patent offered a number of additional technical advantages over prior approaches to network security. As one example, the claimed virtualized network security system (and methods of securing and configuring such a virtualized network security system) reduce or eliminate the substantial expense associated with the hardware security facilities required to physically segment a network and avoid the resulting complexity that may leave segments vulnerable to intrusion. *See id.* at 4:52-62.

94. As another example, the virtualized network security system described and claimed in the ’540 Patent advantageously enables the logical arrangements to be "tailored to the data flows; consistent with a wieldy, logical model (as opposed to an unwieldy, physical model)." *Id.* at 85:23-26. A further improvement afforded by the virtualization is that "the logical arrangements may be applied programmatically, automatically, and/or transparently with respect to a source and/or sink (i.e. a transmitting computing facility and/or a receiving computing facility) of the data flows," and the virtualization may be provided with respect to a data flow as a function of the source and/or destination IP address of the data flow." *Id.* at 85:26-34.

95. As another example, "[v]irtualization of a networked security deployment may also be used to share network security hardware resources such as a firewall among otherwise separate networks." *Id.* at 87:14-16. Associating each separate network with a virtual network allows a network administrator or owner to define a security policy for their network and have the defined security policy applied to network traffic associated with their virtual network. *See id.* at 87:14-21. Advantageously, the claimed invention of the ’540 Patent allows many different kinds of network configurations to be virtualized, such as "individual enterprises leasing security from a security provider." *Id.* at 87:21-24.

96. As another example, virtualization of network security also facilitates improvements in network security. For example, a development virtual network that mirrors a user virtual network may be defined such that internet traffic for the user virtual network also propagates to the development virtual network. *See id.* at 88:11-16. The security policy for the development virtual network can be updated with experimental intrusion prevention techniques that are being tested without causing intrusion or false rejects on the user virtual network. *See id.* at 88:16-19.

97. As another example, virtualization of network security facilitates "load balancing of resources within a flow processing facility" by enabling data flow associated with one virtual network to be routed to one of a plurality of application processor modules while routing data flow associated with another virtual network to another application processor module. *See id.* at 88:20-25.

98. The approaches described and claimed in the '540 Patent represented a significant advance over the prior approaches to network security that were not well-known, routine, or conventional in the field at the time the application which lead to the '540 Patent was filed. On information and belief, during examination of the application which ultimately issued as the '540 Patent, the patent examiner at the USPTO considered at least 64 U.S. and foreign patent documents, as well as 31 other publications. *See id.* at Cover Page. *See also* Ex. P, '540 Patent Prosecution History, at 821, 823-833, 951-952, 954-960, 1157-1161, 1163-1177, 1214-1217, 1227-1228, 1238-1239, 1246 (describing search results and references considered). These include references describing solutions from Microsoft Corporation, IBM, Fujitsu, and Lucent Technologies, amongst others. The patent examiner determined that none disclosed or rendered obvious the inventions of the '540 Patent. *See* Ex. P, '540 Patent Prosecution History, at 1148-1156 (notice of allowance). Indeed, the examiner stated that the "closest" prior art "fails to teach or suggest 'processing the data flow received at said first port for the first and second virtual networks through at least one of the plurality of flow processor processors, wherein portions of the data flow that are associated with the first virtual network are processed according to the first security policy, and wherein portions of the data flow that are associated

with the second virtual network are processed according to the second security policy, said processing further comprising: making a first determination, in accordance with one of the first security policy and the second security policy, of abnormalities that are associated with the data flow, the first determination based at least in part on the subscriber identified by the subscriber profile data; and making a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data, and transferring said data flow to said second port," as described and claimed in the '540 Patent. *Id.* at 1153-1154.

99. On information and belief, Zscaler directly infringes one or more claims of the '540 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

100. Claim 13 of the '540 Patent recites as follows:

> A virtualized network security system (VNSS) comprising:
>
> a plurality of flow processing facilities configured as elements of the VNSS for processing a data flow, said data flow being transferred between a first port and a second port of the VNSS, the data flow comprising subscriber profile data;
>
> a network management facility that is networked with the plurality of flow processing facilities; and
>
> a first security policy for a first virtual network, based at least in part on the subscriber profile data included in the data flow;
>
> a second security policy for a second virtual network, based at least in part on the subscriber profile data included in the data flow, wherein the two or more flow processing facilities receive at least one of the first security policy and the second security policy while receiving said data flow on said plurality of first ports and transferring said data flow to said plurality of second ports,
>
> wherein the plurality of flow processing facilities make a first determination, in accordance with one of the first security policy and the second security policy, of abnormalities that are associated with the data flow, the first determination based at least in part on the subscriber identified by the subscriber profile data; and

> wherein the plurality of flow processing facilities make a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data.

101. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of at least Claim 13. Zscaler's cloud security platform, including its ZEN component, implements policy enforcement by providing a VNSS. For example, Zscaler's cloud security platform creates a global network that acts as a single virtual proxy. Zscaler's cloud security platform, including its ZEN component, includes a plurality of flow processing facilities that are configured as elements of the VNSS for processing a data flow, and the data flow is transferred between a first port and a second port of the VNSS. As an example, Zscaler's ZEN component uses multiple security analysis engines to analyze traffic. Once traffic reaches the ZEN component, the security analysis engines scan the content using, for example, Zscaler's ByteScan technology. Zscaler's cloud security platform, including its ZEN component, also includes a network management facility that is networked with the plurality of flow processing facilities. As an example, Zscaler's cloud security platform, including its CA component, communicates with the ZEN component and directs traffic to the ZEN component. Zscaler's cloud security platform, including its ZEN component, includes a first security policy for a first virtual network, which is based at least in part on the subscriber profile data included in the data flow, and also includes a second security policy for a second virtual network, based at least in part on the subscriber profile data included in the data flow. For example, Zscaler's cloud security platform, including its ZEN component, supports group and user policies being provisioned on the Zscaler database to enable Zscaler's cloud security platform, including its ZEN component, to authenticate the user. Enabling authentication allows Zscaler's cloud security platform, including the ZEN component, to identify the traffic that it receives so it can enforce the configured group and user policies. Zscaler's cloud security platform, including its ZEN component, also enforces policies with user-level granularity based on defining the policies according to a user or a group. Zscaler's cloud security platform, including the ZEN component, includes two or more flow processing facilities that receive at least one of the first

security policy and the second security policy while receiving the data flow on the plurality of first ports and transferring the data flow to the plurality of second ports. For example, Zscaler's cloud security platform, including its ZEN component, receives the content and enforces the security policies served by the CA to implement the group and user policies. Zscaler's cloud security platform includes multiple ZEN components, and the ZEN component includes multiple security analysis engines that scan the content according to the security policies. Zscaler's cloud security platform, including the ZEN component, include the plurality of flow processing facilities to make a first determination, in accordance with one of the first security policy and the second security policy, of abnormalities that are associated with the data flow. For example, Zscaler's cloud security platform, including its ZEN component, uses Zscaler's ByteScan technology to inspect every byte of a request, content, responses, and all related data for inline blocking threats like viruses, cross site scripting, and botnets. As another example, Zscaler's cloud security platform, including its ZEN component, inspects all end user traffic through Single Scan Multi Action technology to ensure security against current and emerging threats based on the user provisioning. Single Scan Multi Action technology subjects the content to every level of inspection unless malicious content is identified at a lower level. Using Zscaler's cloud security platform, including its ZEN component, the first determination is based at least in part on the subscriber identified by the subscriber profile data. The plurality of flow processing facilities makes a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data. As an example, Zscaler's cloud security platform, including its ZEN component, inspects every byte of traffic inline across multiple security techniques and enforces compliance according to granular user policies. Zscaler's cloud security platform may be configured to enforce multiple security policies, including, but not limited to, web security, advanced threats, and anti-virus and anti-spyware.

102. In view of the foregoing, Zscaler directly infringes the '540 Patent in violation of 35 U.S.C. § 271(a).

103. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the ’540 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the ’540 Patent, Zscaler is inducing infringement of the ’540 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler’s marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the ’540 Patent.

104. Symantec has no adequate remedy at law for Zscaler’s acts of infringement. As a direct and proximate result of Zscaler’s acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler’s acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

105. Zscaler without authority supplied or caused to be supplied in or from the United States all or a substantial portion of the components of the invention of the ’540 Patent, where such components are uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the patents if such combination occurred within the United States. For example, Zscaler’s Cloud Security Platform relies upon world-wide data centers. *See, e.g.*, Zscaler, Cloud Architecture Security as a Service, available at https://www.zscaler.com/products/cloud-architecture-security-as-a-service. Zscaler uses servers to enforce security policies in each of the world-wide data centers. *Id.* Zscaler has supplied servers from the United States and installed those servers in foreign data centers. *See, e.g.*, Zscaler, Cloud Enforcement Node Ranges, available at https://ips.zscaler.net/cenr. Zscaler separately transmits its compiled source code from the United States to the servers at data centers outside of the United States. Zscaler actively induces the combination of the servers and the compiled source code at foreign data centers. Zscaler, without permission from Symantec, supplied and/or caused to be supplied in or from the United States all or a substantial portion of the hardware and/or software components of the Zscaler platform (e.g., servers and/or compiled source code), which infringes the ’540 Patent, where such components were uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States (e.g., at Zscaler foreign data

centers) in a manner that would infringe the patents if such combination occurred within the United States. In view of the foregoing, the Zscaler Platform infringes the ’540 Patent in violation of 35 U.S.C. § 271(f)(1).

106. Zscaler without authority supplied or caused to be supplied in or from the United States at least one component of the ’540 patented invention that is especially made or especially adapted for use in the ’540 patented invention and not a staple article or commodity of commerce suitable for substantial noninfringing use, where such component is uncombined in whole or in part, knowing that such component is so made or adapted and intending that such component will be combined outside of the United States in a manner that would infringe the patent if such combination occurred within the United States. For example, Zscaler’s Cloud Security Platform relies upon world-wide data centers. Zscaler, Cloud Architecture Security as a Service, available at https://www.zscaler.com/products/cloud-architecture-security-as-a-service. Zscaler uses servers to enforce security policies in each of the world-wide data centers. *Id*. Zscaler has supplied servers from the United States and installed those servers in foreign data centers. *See, e.g.*, Zscaler, Cloud Enforcement Node Ranges, available at https://ips.zscaler.net/cenr. Zscaler separately transmits its compiled source code from within the United States to the servers in data centers outside of the United States intending to combine the source code with servers in the foreign data centers. Zscaler, without permission from Symantec, supplied and/or caused to be supplied in or from the United States hardware and/or software components (e.g., servers and/or compiled source code) of the Zscaler Platform that—as Zscaler knows—are especially made or especially adapted for use in the ’540 patented invention and are not a staple article or commodity of commerce suitable for substantial non-infringing use, where such components were uncombined in whole or in part, intending that the hardware and/or software components of the Zscaler Cloud Security Platform will be combined outside of the United States (e.g., at Zscaler foreign data centers) in a manner that would infringe the patents if such combination occurred within the United States. In view of the foregoing, the Zscaler Platform infringes the ’540 Patent in violation of 35 U.S.C. § 271(f)(2).

PRAYER FOR RELIEF

WHEREFORE, Symantec prays for judgment in its favor granting the following relief:

A. A finding that Zscaler has directly infringed and/or induced others to infringe the Patents-in-Suit;

B. An award of damages pursuant to 35 U.S.C. § 284 adequate to compensate Symantec for Zscaler's infringement of the Patents-in-Suit, including both pre- and post-judgment interest and costs as fixed by the Court;

C. A preliminary and/or permanent injunction against Zscaler and its officers, agents, servants, employees, and representatives, and all others in active concert or participation with them, from further infringing the Patents-in-Suit;

D. A finding that Zscaler's infringement of at least the '429 Patent and '446 Patent has been willful.

E. A declaration that this is an exceptional case within the meaning of 35 U.S.C. § 285, and a corresponding award of Symantec's reasonable attorney fees incurred in connection with the litigation; and

F. Any additional and further relief the Court may deem just and proper under the circumstances.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b) and District of Delaware Local Rule 38.1, Plaintiffs hereby demand a trial by jury on all issues so triable

Dated: November 14, 2019

Respectfully submitted,
BAKER BOTTS L.L.P.

/s/ *Kurt M. Pankratz*
Kurt M. Pankratz

Attorneys for Symantec Corporation
and Symantec Limited.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a) on November 14, 2019. As such, this document was served on all counsel who have consented to electronic service.

/s/ Kurt M. Pankratz
Kurt M. Pankratz