UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FIRENET TECHNOLOGIES, LLC,	
Plaintiff,	**Case No.: ____________**
v.	**DEMAND FOR JURY TRIAL**
CITRIX SYSTEMS, INC.,	
Defendant.	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff FireNet Technologies, LLC ("FireNet" or "Plaintiff"), by way of this Complaint against Citrix Systems, Inc. ("Citrix" or "Defendant"), alleges as follows:

PARTIES

1. Plaintiff FireNet is a limited liability company organized and existing under the laws of the State of Georgia, having its principal place of business at Day Building, Suite 230, 4725 Peachtree Corners Circle, Peachtree Corners, GA 30092.

2. On information and belief, Defendant Citrix is a Delaware corporation, having its principal place of business at 851 West Cypress Creek Rd, Fort Lauderdale, FL, 33309.

3. On information and belief, Citrix is registered to do business in the

State of Georgia with a physical address 40 Technology Parkway South, Suite 300, Norcross, GA, 30092.

4. On information and belief, Defendant Citrix has a physical office in this judicial district located at 13560 Morris Road #2500, Alpharetta, GA 3004.

JURISDICTION AND VENUE

5. This is an action under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.*, for infringement by Citrix of U.S. Patent No's. 6,317,837; 7,739,302; 8,306,994; and 8,892,600 ("Patents-in-Suit").

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

7. Citrix is subject to the personal jurisdiction of this Court because, *inter alia*, on information and belief, (i) Citrix is registered to conduct and transacts business in the State of Georgia; and (ii) Citrix has committed and continues to commit acts of patent infringement in the State of Georgia, including by making, using, offering to sell, and/or selling accused products and services in the State of Georgia, and/or importing accused products and services into the State of Georgia, and (iii) Citrix owns, uses, or possesses real property situated in the State of Georgia.

8. Venue is proper as to Citrix in this district pursuant to 28 U.S.C. §

1400(b) because, *inter alia*, on information and belief, Citrix maintains a regular and established place of business in this judicial district, and Citrix has committed and continues to commit acts of patent infringement in this judicial district, including by making, using, offering to sell, and/or selling accused products and services in this district, and/or importing accused products and services into this district.

BACKGROUND

9. On November 13, 2001, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 6,317,837, entitled "Internal Network Node With Dedicated Firewall" (the "'837 Patent"). A copy of the '837 Patent is attached hereto as Exhibit A.

10. On June 15, 2010, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 7,739,302, entitled "Network Attached Device With Dedicated Firewall Security" (the "'302 Patent"). A copy of the '302 Patent is attached hereto as Exhibit B.

11. On November 6, 2012, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 8,306,994, entitled "Network Attached Device With Dedicated Firewall Security" (the "'994 Patent"). A copy of the '994 Patent is attached hereto as Exhibit C.

12. On November 18, 2014, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 8,892,600, entitled "Network Attached Device With Dedicated Firewall Security" (the "'600 Patent"). A copy of the '600 Patent is attached hereto as Exhibit D.

13. FireNet is the assignee and owner of the right, title, and interest in and to the Patents-in-Suit, including the right to assert all causes of action arising under said patents and the right to any remedies for infringement.

NOTICE

14. By letter dated April 12, 2018, FireNet notified Citrix of the existence of the Patents-in-Suit, and of infringement thereof by Citrix and Citrix's customers. FireNet's letter identified exemplary infringing Citrix's products and an exemplary infringed claim for each of the Patents-in-Suit. FireNet's April 12, 2018 letter invited Citrix to hold a licensing discussion with FireNet.

15. By letter dated January 23, 2019, FireNet again notified Citrix of the existence of the Patents-in-Suit, and of infringement thereof by Citrix and Citrix's customers. FireNet's follow-up letter again identified exemplary infringing Citrix products and an exemplary infringed claim for each of the Patents-in-Suit. FireNet's January 23, 2019 letter again invited Citrix to hold a licensing discussion with FireNet.

16. As of the date of this Complaint, FireNet has not received any response from Citrix to its letters.

COUNT I: INFRINGEMENT OF THE '837 PATENT

17. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

18. On information and belief, Citrix has infringed the '837 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, selling in the United States or importing into the United States Citrix networking products and services, including, but not limited to, NetScaler ADC (also referred to as Citrix ADC) products, including hardware appliances (MPX and SDX), software implementations (VPX and CPX), and cloud implementations ("Accused Products").

19. For example, on information and belief, Citrix has infringed at least claim 37 of the '837 Patent by performing a method of managing access to a network attached device (NAD) in a network arrangement including a first group of nodes defining an internal network and a second group of nodes defining an external network. A network arrangement that uses Accused Products to manage access to nodes ("Citrix Network") has a first group of nodes, such as, for example, servers and clients on an internal corporate network, and a second group of nodes,

such as client computers accessing the various servers over the Internet (external network). Ex. E, NetScaler 12.0 at 18. In the network arrangement, the external network is connected in communication with the internal network by an intermediate node including a bastion firewall (such as the NetScaler external firewall) for protecting the nodes of the internal network from unauthorized communication originating at external nodes. Ex. F, Citrix NetScaler Gateway and Citrix Desktops & Apps, The Ultimate How-To Guide for Successful Deployments, Slide 8. The internal network includes the NAD, such as a hard-drive storage array residing on a server. *See* Ex. E at 18. The Accused Products, using their firewall functionality, determine for each and every request for network access to the NAD, such as a packet requesting information stored on a NAD, whether each request for network access to said NAD is authorized. The Accused Products provide network access to said NAD when a request is authorized. The Accused Products deny network access to said NAD when a request is not authorized. In the Citrix Network, the NAD is protected by a dedicated NAD firewall from unauthorized network access requests originating at the intermediate and internal and external nodes of the network arrangement. *See, e.g.,* Ex. E at 2888 ("Access Control Lists (ACLs) filter IP traffic and secure your network from unauthorized access. An ACL is a set of conditions that the NetScaler ADC evaluates to determine whether to allow access. For example, the Finance department probably does not want to allow its resources to be accessed by other departments, such as HR and Documentation, and those departments want to restrict access to their data.”).

20. On information and belief, Citrix has induced infringement of the ’837 Patent pursuant to 35 U.S.C. § 271(b), by actively and knowingly inducing, directing, causing, and encouraging others, including, but not limited to, its partners, software developers, customers, and end users, to make, use, sell, and/or offer to sell in the United States, and/or import into the United States, the Accused Products by, among other things, providing instructions, manuals, and technical assistance relating to the installation, set up, use, operation, and maintenance of said products, such as deployment guides, installation guides, and instructional videos, all available at the Citrix website.

21. On information and belief, Citrix has committed the foregoing infringing activities without a license.

22. On information and belief, Citrix’s infringing activities have occurred within the six years prior to the filing of the original complaint in this action, entitling FireNet to past damages.

23. On information and belief, Citrix knew the ’837 Patent existed while

committing the foregoing infringing acts, thereby willfully, wantonly and deliberately infringing the ’837 Patent.

COUNT II: INFRINGEMENT OF THE ’302 PATENT

24. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

25. On information and belief, Citrix has infringed the ’302 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, selling in the United States or importing into the United States the Accused Products.

26. For example, on information and belief, Citrix has infringed at least claim 1 of the ’302 Patent by making, using, offering to sell, selling in the United States or importing into the United States a network arrangement comprising a network client and at least one network attached device (NAD) residing on a same network. A network arrangement that uses Accused Products to manage access to nodes (“Citrix Network”) has, for example, at least one client and one hard-disk storage array residing on a server, both of which reside on the same corporate network. Ex. E at 2710 (“For an improved performance in the delivery of virtual desktop applications, you can integrate the NetScaler appliance with Citrix XenDesktop”) and at 2888 (“Access Control Lists (ACLs) filter IP traffic and

secure your network from unauthorized access. An ACL is a set of conditions that the NetScaler ADC evaluates to determine whether to allow access. For example, the Finance department probably does not want to allow its resources to be accessed by other departments, such as HR and Documentation, and those departments want to restrict access to their data.”). In the Citrix Network, a NAD server is disposed between the network client and the NAD. For example, the access control functionality of the Citrix NetScaler is disposed between a client and the server with a hard drive array. *Id* at 18. In the Citrix Network, the NAD server is configured to electronically communicate with the NAD over a connection. For example, the NetScaler is configured to communicate with the hard drive array residing in a server, such as XenDesktop, via an interface. The NAD server is further configured to receive a request contained in a data packet for network access to the NAD. In the Citrix Network, the NetScaler is configured to receive a request, contained in, for example, a TCP/IP packet, to access the storage array residing on a server. The NAD server includes computer executable instructions that, upon execution, cause the NAD server to determine whether the header of a received data packet containing the request for network access includes at least one of an IP address of a network source, an IP address of a network destination, and a route of the data packet. NetScaler includes executable instructions that processes incoming packets to determine, among others, the presence of an IP Source Address field. The NAD is further configured to filter the data packet based at least on an IP address in a header of the data packet. For example, a storage array residing inside a server is configured to use, for example, the integrated access control functionality to filter the data packets based on, for example, the IP Source Address field in the packet header. Upon execution, the computer executable instructions further cause the NAD server to determine whether the received request for network access to the NAD is authorized. Upon execution, the executable instructions cause XenDesktop server to determine whether to allow or deny a packet based on various information, i.e., determine whether the request is authorized. Upon execution, the computer executable instructions provide the network client with network access to the NAD only if the request for network access is authorized, such that the NAD is protected from unauthorized access requests from the network client and other devices in a manner that is in addition to any protection afforded by a firewall. In addition to the protection afforded by an edge firewall, the instructions executing on NetScaler provide the network client, and other network devices, such as Internet clients, with access to servers with hard drive arrays only if the requests are authorized.

27. On information and belief, Citrix has induced infringement of the

’302 Patent pursuant to 35 U.S.C. § 271(b), by actively and knowingly inducing, directing, causing, and encouraging others, including, but not limited to, its partners, software developers, customers, and end users, to make, use, sell, and/or offer to sell in the United States, and/or import into the United States, the Accused Products by, among other things, providing instructions, manuals, and technical assistance relating to the installation, set up, use, operation, and maintenance of said products, such as deployment guides, installation guides, and instructional videos, all available at the Citrix website.

28. On information and belief, Citrix has committed the foregoing infringing activities without a license.

29. On information and belief, Citrix’s infringing activities have occurred within the six years prior to the filing of the original complaint in this action, entitling FireNet to past damages.

30. On information and belief, Citrix knew the ’302 Patent existed while committing the foregoing infringing acts, thereby willfully, wantonly and deliberately infringing the ’302 Patent.

COUNT III: INFRINGEMENT OF THE ’994 PATENT

31. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

32. On information and belief, Citrix has infringed the ’994 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, selling in the United States or importing into the United States the Accused Products.

33. For example, on information and belief, Citrix has infringed at least claim 10 of the ’994 Patent by performing a method comprising processing, by a network attached device (NAD) server coupled to an internal network, a request for network access to a NAD device. An Accused Product, such as NetScaler, including hardware appliances, software implementations, and cloud implementations, is coupled to an internal local area network (LAN). Ex. E at 18. NetScaler processes a request for network access to, for example, a hard-drive storage array residing on a server. The NAD device is coupled to the NAD server and configured to receive communication from an internal network only by way of the NAD server. For example, the hard-drive storage array residing on a server (the NAD device) is coupled to NetScaler and the NAD device is configured to receive communications only through NetScaler. *See* Ex. E at 2888 (“Access Control Lists (ACLs) filter IP traffic and secure your network from unauthorized access. An ACL is a set of conditions that the NetScaler ADC evaluates to determine whether to allow access. For example, the Finance department probably

does not want to allow its resources to be accessed by other departments, such as HR and Documentation, and those departments want to restrict access to their data.”). The request for network access includes a data packet that includes at least an IP header. For example, the request for network access is a TCP/IP packet that includes an IP header. The NAD server comprises a NAD server firewall. For example, NetScaler includes access control functionality which protects the hard-drive storage array server from undesirable requests. Citrix determines, by the NAD server firewall such as NetScaler access control function, whether the request for network access to the NAD should be authorized or denied based on a filtering of at least the IP header of the data packet of the received request for network access to the NAD. By using the access control functionality in the Accused Products, Citrix determines whether the request for accessing the server storage array should be authorized or denied, such as based on a filtering of the IP header of the data packet with the request. Citirx processes, by the NAD server, the data packet for communication with the NAD and enables access to the NAD upon determining that the requested network access to the NAD should be authorized. For example, the Accused Products, process the data packet for communication with the hard-drive storage array server and enable access to the server when a request is determined as authorized. Citrix blocks, by the NAD server, access to the NAD upon determining that the request for network access to the NAD should be denied. For example, the Accused Products block the request for accessing the storage array residing in a server, if the Citrix determines that the request should be denied.

34. On information and belief, Citrix has induced infringement of the ’994 Patent pursuant to 35 U.S.C. § 271(b), by actively and knowingly inducing, directing, causing, and encouraging others, including, but not limited to, its partners, software developers, customers, and end users, to make, use, sell, and/or offer to sell in the United States, and/or import into the United States, the Accused Products by, among other things, providing instructions, manuals, and technical assistance relating to the installation, set up, use, operation, and maintenance of said products, such as deployment guides, installation guides, and instructional videos, all available at the Citrix website.

35. On information and belief, Citrix has committed the foregoing infringing activities without a license.

36. On information and belief, Citrix’s infringing activities have occurred within the six years prior to the filing of the original complaint in this action, entitling FireNet to past damages.

37. On information and belief, Citrix knew the ’994 Patent existed while

committing the foregoing infringing acts, thereby willfully, wantonly and deliberately infringing the ’994 Patent.

COUNT IV: INFRINGEMENT OF THE ’600 PATENT

38. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

39. On information and belief, Citrix has infringed the ’600 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, selling in the United States or importing into the United States the Accused Products.

40. For example, on information and belief, Citrix has infringed at least claim 8 of the ’600 Patent by performing a computer-implemented method as set forth in the claim. Specifically, Citrix receives, by a first computing device coupled to an internal network, data packets over the internal network. Ex. E at 2888. In the Citrix Network, an Accused Product such as NetScaler products, including hardware appliances, software implementations, and cloud implementations, connected to an internal local area network (LAN) receives data packets over the LAN. *Id.* At least some of the data packets are sent to the internal network from an external network. *Id.* At least some of these packets are sent by an external network, such as devices outside the Citrix Network connected

to the Internet. Citrix examines, by the first computing device, the data packets to determine whether the data packets contain an IP address associated with an attached device coupled to a second computing device. *Id.* For example, the Accused Product, such as NetScaler, examines the data packets to determine whether they contain an IP address associated with an attached device, such as a hard-drive storage array, coupled to a second attached device, such as the storage-array server. In the Citrix Network, the second computing device is in communication with the first computing device and the second computing device is isolated from the internal network. *Id.* For example, the server hosting the hard-disk storage array is in communication with NetScaler and the server is not accessible to other devices, except through NetScaler. *See* Ex. E at 2888 ("Access Control Lists (ACLs) filter IP traffic and secure your network from unauthorized access. An ACL is a set of conditions that the NetScaler ADC evaluates to determine whether to allow access. For example, the Finance department probably does not want to allow its resources to be accessed by other departments, such as HR and Documentation, and those departments want to restrict access to their data."). Citrix filters, by the first computing device, data packets by determining whether the IP address in a header of the data packets is valid to determine whether to authorize data packets containing information indicative of a request for access to the attached device. The Accused Products filter data packets by determining based on the IP address in the packet header, whether to authorize information indicative of the request in the packet for access of the hard drive or other memory of the server. Citrix reformulates, by the first computing device, the data packets for communication to the second computing device coupled to the attached device in response to authorizing the data packets containing the information indicative of the request for access to the attached device. For example, in response to authorizing the data packets containing information indicative of the request for access of the hard-drive storage array or other memory of a server device, the Accused Product, such as NetScaler, reformulates the data packets by changing an address field in the header of the packet, for communication with the server device that is coupled to the hard drive or the other memory.

41. On information and belief, Citrix has induced infringement of the ’600 Patent pursuant to 35 U.S.C. § 271(b), by actively and knowingly inducing, directing, causing, and encouraging others, including, but not limited to, its partners, software developers, customers, and end users, to make, use, sell, and/or offer to sell in the United States, and/or import into the United States, the Accused Products by, among other things, providing instructions, manuals, and technical assistance relating to the installation, set up, use, operation, and maintenance of

said products, such as deployment guides, installation guides, and instructional videos, all available at the Citrix website.

42. On information and belief, Citrix has committed the foregoing infringing activities without a license.

43. On information and belief, Citrix's infringing activities have occurred within the six years prior to the filing of the original complaint in this action, entitling FireNet to past damages.

44. On information and belief, Citrix knew the '600 Patent existed while committing the foregoing infringing acts, thereby willfully, wantonly and deliberately infringing the '600 Patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff FireNet prays for the judgment in its favor against Citrix, and specifically, for the following relief:

A. Entry of judgment in favor of FireNet against Citrix on all counts;

B. Entry of judgment that Citrix has infringed the Patents-in-Suit;

C. Entry of judgment that Citrix's infringement of the Patents-in-Suit has been willful;

D. Award of compensatory damages adequate to compensate FireNet for Citrix's infringement of the Patent-in-Suit, in no event less than a reasonable royalty trebled as provided by 35 U.S.C. § 284;

E. Declaration and finding that Citrix's conduct in this case is exceptional under 35 U.S.C. § 285;

F. Award of reasonable attorneys' fees and expenses against Citrix pursuant to 35 U.S.C. § 285;

G. Award of FireNet's costs;

H. Pre-judgment and post-judgment interest on FireNet's award; and

I. All such other and further relief as the Court deems just or equitable.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Fed. R. Civ. P., Plaintiff FireNet hereby demands trial by jury in this action of all claims so triable.

Dated: July 12, 2019

Respectfully submitted,

/s/*Daniel A. Kent*
Daniel A. Kent
Georgia Bar No. 415110
Kent & Risley LLC
5755 N Point Pkwy Ste 57
Alpharetta, GA 30022
Ph: 404-585-4214
Fx: 404-829-2412
Em: dankent@kentrisley.com

Dmitry Kheyfits
(*pro hac vice* to be filed)
dkheyfits@kblit.com
KHEYFITS BELENKY LLP
4 Embarcadero Center, Suite 1400
San Francisco, CA 94111
Tel: 415-429-1739
Fax: 415-429-6347

Andrey Belenky
(*pro hac vice* to be filed)
abelenky@kblit.com
Hanna G. Cohen
(*pro hac vice* to be filed)
hgcohen@kblit.com
KHEYFITS BELENKY LLP
1140 Avenue of the Americas, 9th Floor
New York, NY 10036
Tel: 212-203-5399
Fax: 212-203-5399

Attorneys for Plaintiff
FireNet Technologies, LLC