

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

LONGHORN HD LLC.,

Plaintiff,

v.

CHECK POINT SOFTWARE
TECHNOLOGIES LTD.,

Defendant.

§
§
§
§
§
§
§
§
§
§
§
§

Case No.

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Longhorn HD LLC. (“LHD” or “Plaintiff”) for its Complaint against Defendant Check Point Software Technologies Ltd. (“Check Point” or “Defendant”) alleges as follows:

THE PARTIES

1. LHD is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located at 203 East Travis Street, Marshall, Texas 75670

2. Upon information and belief, Defendant Check Point Software Technologies Ltd. is corporation organized under the laws of the Country of Israel, with its principal place of business at Shlomo Kaplan St 5, Tel Aviv-Yafo, 6789159, Israel. Upon information and belief, Defendant may be served pursuant to the provisions of the Hague Convention. Upon information and belief, Check Point does business in Texas and in the Eastern District of Texas, directly or through intermediaries.

JURISDICTION

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.* This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

5. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because, among other things, Defendant is a defendant not resident in the United States, and thus may be sued in any judicial district pursuant to 28 U.S.C. § 1391(c)(3).

6. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

7. On July 16, 2002, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 6,421,732 (the "'732 Patent") entitled "IPNet Gateway." A true and correct copy of the '732 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=6421732>.

8. On November 4, 2003, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 6,643,778 (the “’778 Patent”) entitled “Network System Using A Firewall Dynamic Control Method.” A true and correct copy of the ’778 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=6643778>.

9. On October 11, 2005, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 6,954,790 (the “’790 Patent”) entitled “Network-Based Mobile Workgroup System.” A true and correct copy of the ’790 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=6954790>.

10. On August 21, 2007, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,260,846 (the “’846 Patent”) entitled “Intrusion Detection System.” A true and correct copy of the ’846 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=7260846>.

11. On March 11, 2008, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,343,421 (the “’421 Patent”) entitled “Restricting Communication of Selected Processes to a Set of Specific Network Addresses.” A true and correct copy of the ’421 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=7343421>.

12. LHD is the sole and exclusive owner of all right, title, and interest in the ’732 Patent, the ’778 Patent, the ’790 Patent, the ’846 Patent, and the ’421 Patent (collectively, the “Patents-in-Suit”), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. LHD also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

FACTUAL ALLEGATIONS

13. The Patents-in-Suit generally cover systems and methods for computer and network security.

14. The '732 Patent generally relates to technology for mapping resources on private networks to public facing domain names. The technology described by the '732 Patent generally relates to technology that maps multiple resources and/or addresses on a private network to addresses for external use, such as mapping multiple internal resources to a single IP address to work with a Domain Name Service (“DNS”) lookup. The technology further implements these mappings as the basis for a secure firewall. The technology described in the '732 Patent was developed by Hasan Alkhatib and Bruce Wooton at IP Dynamics, Inc. By way of example, this technology is implemented today in network firewalls and gateways that allow remote users to access multiple resources with shared domains/IP addresses.

15. The '778 Patent generally relates to technology for remotely connecting to a first Intranet and accessing information on a second Intranet. The technology further implements these mappings as the basis for secure gateways. The technology described in the '778 Patent was developed by Osamu Nakazawa at Oki Electric Industry Co., Ltd. By way of example, this technology is implemented today in network firewalls and gateways that allow IP Security (“IPSec”) over virtual private networks (“VPN”) for sharing of resources among intranets.

16. The '790 Patent generally relates to technology for mobile workgroups' VPN and firewall systems. The technology further implements these mappings as the basis for secure gateways. The technology described in the '790 Patent was developed by Jan Forsl w at Interactive People Unplugged AB. By way of example, this technology is implemented today in

VPNs that allow for mobile participation, further implementing network firewalls and gateways that allow for the VPNs to share resources with mobile devices.

17. The '846 Patent generally relates to technology for intrusion detection systems. The technology described in the '846 Patent was developed by Christopher Day at Steelcloud, Inc. By way of example, this technology is implemented today in intrusion detection systems (“IDS”) and intrusion prevention systems (“IPS”) that utilize machine-learning techniques to detect and prevent intrusions.

18. The '421 Patent generally relates to technology that solves problems endemic to the computer server and networking fields. More specifically, the inventions disclosed in the '421 Patent provide advancements in the field of computer server virtualization, resource sharing, and security through the use of methods for restricting network address-based communication. The technology described in the '421 Patent was developed by Pawan Goyal at Digital Asset Enterprises LLC. By way of example, this technology is implemented today in gateway and firewall devices to allow or disallow resources for computer processes on ports so as to provide advancements in computer security and resource management.

19. Check Point has infringed and is continuing to infringe one or more of the Patents-in-Suit by making, using, selling, offering to sell, and/or importing, and by actively inducing others to make, use, sell, offer to sell, and/or importing, products that include security gateways, routers, control system security appliance, clouds, and components and software that provide firewall, VPN, IPSec, DNS, IDS/IPS, and selective network address-based communication, mobile security, and threat protection functionality that infringes the Patents-in-Suit (“Accused Products”) including, but not limited to, Check Point Next Generation Firewalls (“NGFWs”), Security Gateway devices, and Network Threat Prevention devices and services,

including, for example, Series Services Gateways including, for example. The Check Point R75, R76, R77, R80¹, E80, 1400 Series Appliances, 700 Series Appliances, 900 Series Appliances, 1500 Series Appliances, 1200R Rugged Appliances, 3000 Appliances, 5000 Appliances, 6000 Appliances, 15000 Appliances, 16000 Appliances, 23000 Appliances, 26000 Appliances, 44000 and 64000 Security Systems, and CloudGuard Appliances, SandBlast Appliances, Check Point Infinity, GAIA operating system, utilities, and software.

COUNT I
(Infringement of the '732 Patent)

20. Paragraphs 1 through 19 are incorporated by reference as if fully set forth herein.

21. LHD has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '732 Patent.

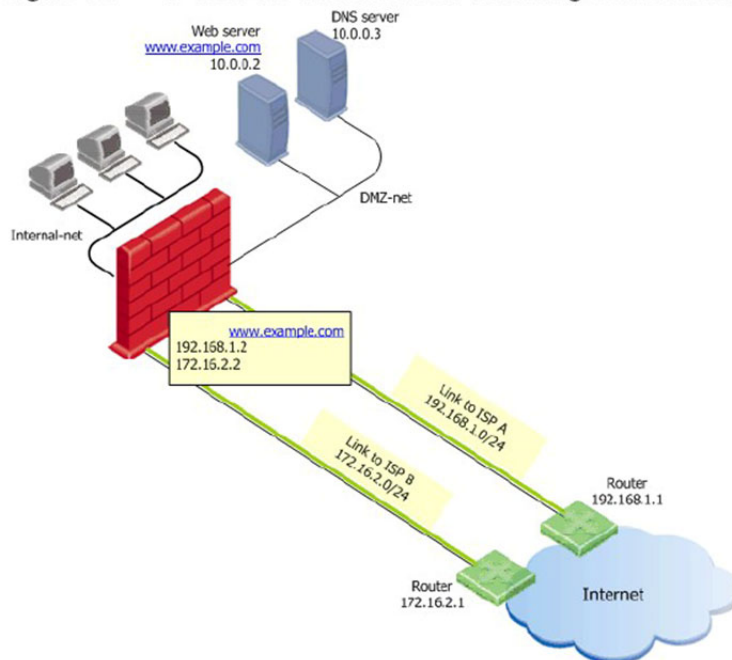
22. Defendant has directly infringed the '732 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that meet each and every limitation of one or more claims of the '732 Patent including by performing the methods claimed by the '732 Patent. Such products include routers, firewalls, and wide area network utilities that utilize DNS and IP address translation and forwarding. On information and belief, such Check Point products include at least the Accused Products and services that implement DNS and IP address translation and forwarding.

23. For example, Defendant has directly infringed at least claim 1 of the '732 Patent by making, using, offering to sell, selling, and/or importing into the United States products that practice the methods of the '732 Patent including DNS with network translation and IP failover.

¹ See, e.g., http://dl3.checkpoint.com/paid/f9/f91c6c1c7cfd630a5ef2d5b769368bd8/Check_Point_R7x_xx_R8x_xx_Backward_Maps_May_2019.pdf?HashKey=1574044374_23e9f9870ffe3e704ffa9b1578a1d234&xtn=.pdf

24. On information and belief, the Accused Products, including but not limited to the R70 and R80 products perform a method for establishing communication with a first entity inside a network. The Accused Products receive a first address request originating from outside the network. The first address request includes a request of an address of a first entity, identifying the first entity with a domain name for said first entity.²

Figure 4-2 IP Address Resolution for Incoming Connections



The following is a workflow, based on [Figure 4-2](#), of how an incoming connection is established:

1. When a user in the Internet contacts [www.example.com](#), the client machine sends a DNS query for the IP address. The DNS query reaches the Security Gateway. Check Point Security Gateway has a built-in mini-DNS server that can be configured to intercept DNS queries (of type A) for servers in its domain.

25. The Accused Products respond to the first address request by providing a first address that is not unique to said first entity within the network, i.e. the address of the gateway unit. This address is not unique to the first entity in the network as it represents both devices (e.g., example.com). The Accused Products receive requests for communication with the server

² http://supportcontent.checkpoint.com/documentation_download?ID=8738

from entities originating outside the network and establishes communication between the two entities as a forwarder of information.

26. Additionally, the Accused Products perform the method of the claims at least during the process of Internet Service Provider (“ISP”) failover and load balancing where a DNS request is intercepted by the Accused Products and a different IP address corresponding to a second ISP is returned in response to the DNS request.

27. LHD has suffered damages as a result of Defendant’s infringement of the ’732 Patent in an amount to be proved at trial.

COUNT II
(Infringement of the ’778 Patent)

28. Paragraphs 1 through 19 are incorporated by reference as if fully set forth herein.

29. LHD has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’778 Patent.

30. Defendant has directly infringed the ’778 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that meet each and every limitation of one or more claims of the ’778 Patent including by performing the methods claimed by the ’778 Patent. Such products include routers, firewalls, and wide area network utilities that utilize DNS and IP address translation and forwarding. On information and belief, such Check Point products include at least the gateway and firewall products and services that implement IPSec and VPN to connect two gateways.

31. For example, Defendant has directly infringed at least claim 1 of the ’778 Patent by making, using, offering to sell, selling, and/or importing into the United States products that meet each limitation of claim 1 of the ’778 Patent.

32. For example, Defendant has directly infringed at least claim 1 of the '778 Patent by making, using, offering to sell, selling, and/or importing into the United States products that include a network system using a firewall dynamic control method. The Accused Products include a first Intranet connected to a unit and a second Intranet connected to a second unit with the Internet as a base, as depicted in the figure below.³

The Check Point Solution for VPN

A *Virtual Private Network (VPN)* is a secure connectivity platform that both *connects* networks and *protects* the data passing between them. For example, an organization may have geographically spaced networks connected via the Internet; the company has connectivity but no privacy. Check Point Security Gateways provide privacy by encrypting those connections that need to be secure. Another company may connect all parts of its geographically spaced network through the use of dedicated leased lines; this company has achieved connectivity and privacy but at great expense. The Check Point Product Suite offers a cheaper connectivity solution by connecting the different parts of the network via the public Internet.

A Virtual Private Network is a network that employs encrypted tunnels to exchange securely protected data. Check Point Security gateways create encrypted tunnels by using the *Internet Key Exchange (IKE)* and *IP Security (IPSec)* protocols. IKE creates the VPN tunnel, and this tunnel is used to transfer IPSec encoded data.

Think of IKE as the process that builds a tunnel, and IPSec packets as trucks that carry the encrypted data along the tunnel.

Figure 7-1 Simplified VPN tunnel



33. The Accused Products include a first dynamic proxy server (e.g., the Check Point unit at the first Security Gateway depicted in the figure above) for forming a firewall to protect said first Intranet. The Accused Products further include a second dynamic proxy server (e.g., the unit depicted as the second Security Gateway) for forming a firewall to protect the second Intranet.

³ Check Point R70 Power-1 Administration Guide.
https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/8951/FILE/CP_R70_Power-1_AdminGuide.pdf

34. The Accused Products further include a remote access terminal connected to said first Intranet, e.g., the SSL VPN user.⁴

35. The Accused Products include a first object directory server provided within the first Intranet for judging whether a service requested by said remote access terminal is provided in said first Intranet or is provided in said second Intranet.

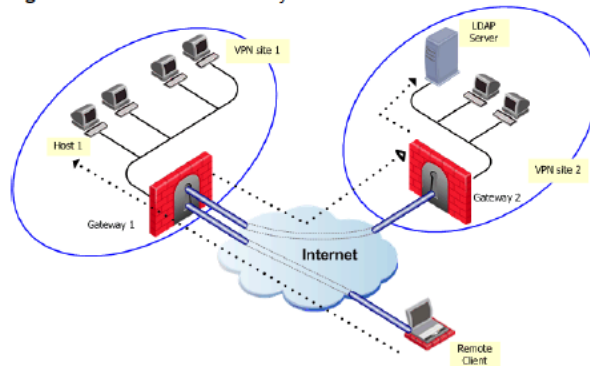
Establishing a Connection Between a Remote User and a Gateway

To allow the user to access a network resource protected by a security gateway, a VPN tunnel establishment process is initiated. An IKE (Internet Key Exchange) negotiation takes place between the peers.

During IKE negotiation, the peers' identities are authenticated. The gateway verifies the user's identity and the client verifies that of the gateway. The authentication can be performed using several methods, including digital certificates issued by the Internal Certificate Authority (ICA). It is also possible to authenticate using third-party PKI solutions, pre-shared secrets or third party authentication methods (for example, SecurID, RADIUS *etc.*).

After the IKE negotiation ends successfully, a secure connection (a VPN tunnel) is established between the client and the gateway. All connections between the client and the gateway's VPN domain (the LAN behind the gateway) are encrypted inside this VPN tunnel, using the IPSec standard. Except for when the user is asked to authenticate in some manner, the VPN establishment process is transparent.

Figure 8-1 Remote to Gateway



In Figure 8-1, the remote user initiates a connection to gateway 1. User management is not performed via the VPN database, but an LDAP server belonging to VPN Site 2. Authentication takes place during the IKE negotiation. Gateway 1 verifies that the user exists by querying the LDAP server behind gateway 2. Once the user's existence is verified, the gateway then authenticates the user, for example by validating the user's certificate. Once IKE is successfully completed, a tunnel is created; the remote client connects to Host 1.

⁴ *Id.*

⁵ *Id.* at 217.

For example, the Security Gateway in the figure above includes a directory of resources including policies and objects available on the Intranets. The Accused Products further include a second object directory server provided in the second Intranet to dynamically install a service proxy in said second dynamic proxy server when said service is provided in said second Intranet. For example, the Security Gateway in the figure above includes a second object directory server to dynamically install a service proxy. The services and objects provided by the unit can be dynamic. Furthermore, on information and belief, the first object directory server includes references to services stored in the first Intranet and makes requests for searches of services provided in said second Intranet to said second dynamic proxy server.

36. LHD has suffered damages as a result of Defendant's direct infringement of the '778 Patent in an amount to be proved at trial.

COUNT III
(Infringement of the '790 Patent)

37. Paragraphs 1 through 19 are incorporated by reference as if fully set forth herein.

38. LHD has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '790 Patent.

39. Defendant has and continues to directly infringe the '790 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '790 Patent. Such products include gateway units which provide a mobile user workgroup.

40. For example, Defendant has and continues to directly infringe at least claim 1 of the '790 Patent by making, using, offering to sell, selling, and/or importing into the United States products that include gateway devices that provide mobile user workgroups. The infringing

systems include a network-based mobile workgroup system comprising a plurality of mobile client nodes, each mobile client node providing an interface for user interaction by a mobile user, for example, Check Point Remote Access Clients running on mobile devices, including but not limited to Android devices.⁶

41. The Accused Products include a plurality of mobile service router nodes, each mobile service router node providing a mobile Virtual Private Network (VPN) to the mobile client nodes spanning multiple router hops and sites, for example, a Check Point Gateway or Firewall unit in connection with access points. The Accused Products further include a network address identifier (NAI) with which a user of a mobile client is uniquely identified to the mobile VPN system, for example, a device Media Access Control (“MAC”) address.

42. Additionally, the Accused Products include a set of firewall filters and route policies with which the workgroup is protected, such as, for example, firewalls and rules enforced by the Check Point Gateway or Firewall units. Additionally, the mobile VPN provides each mobile client secure data access to the VPN and provides secure data access to each mobile client from within the mobile VPN, wherein a point of attachment of any mobile client node to the mobile VPN may change without affecting that mobile client node’s participation in the mobile VPN.

43. Defendant has and continues to indirectly infringe one or more claims of the ’790 Patent by knowingly and intentionally inducing others, including Check Point customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as Check Point client for mobile devices.

⁶ See, e.g., https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101313

44. Defendant, with knowledge that these products, or the use thereof, infringe the '790 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '790 Patent by providing these products to end users for use in an infringing manner.

45. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the '790 Patent, but while remaining willfully blind to the infringement.

46. LHD has suffered damages as a result of Defendant's direct and indirect infringement of the '790 Patent in an amount to be proved at trial.

47. LHD has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '790 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT IV
(Infringement of the '846 Patent)

48. Paragraphs 1 through 19 are incorporated by reference as if fully set forth herein.

49. LHD has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '846 Patent.

50. Defendant has and continues to directly infringe the '846 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '846 Patent. Such products include intrusion detection systems and intrusion prevention systems including the Check Point IDP, Check Point IPS, and Check Point Infinity appliances and devices.

51. For example, Defendant has and continues to directly infringe at least claim 7 of the '846 Patent by making, using, offering to sell, selling, and/or importing into the United States products that include IDS and/or IPS systems that practice the claimed method alone, or in combination with other Check Point products or services.

52. The Accused Products are systems that perform an intrusion detection method comprising the steps of monitoring network traffic passing across a network communications path. For example, the Check Point IPS monitors network traffic. Additionally, Check Point performs network traffic parsing.⁷

53. Additionally, the Accused Products store individual components of said network packets in a database and construct multi-dimensional vectors from at least two of said stored individual components and applying at least one multi-variate analysis to said constructed multi-dimensional vectors, said at least one multi-variate analysis producing a corresponding output set. For example, machine learning techniques are applied to captured packets and signatures, such as with Check Point CADET Technology.⁸ Additionally, the Accused Products establish a correlation between individual output sets based upon a selected metric to identify anomalous behavior.

54. The Accused Products classify the anomalous behavior as an event selected from the group consisting of a network fault, a change in network performance, and a network attack.

55. Defendant has and continues to indirectly infringe one or more claims of the '846 Patent by knowingly and intentionally inducing others, including Check Point customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making,

⁷ https://www.checkpoint.com/downloads/product-related/whitepapers/IPS_Engine_Architecture.pdf

⁸ <https://community.checkpoint.com/t5/IPS-Anti-Virus-Anti-Bot-Anti/Context-Aware-Detection-CADET-is-now-in-production/td-p/26858> Check Point
<https://research.checkpoint.com/about-us/>

using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as IDS and IPS systems.

56. Defendant, with knowledge that these products, or the use thereof, infringe the '846 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '846 Patent by providing these products to end users for use in an infringing manner.

57. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the '846 Patent, but while remaining willfully blind to the infringement.

58. LHD has suffered damages as a result of Defendant's direct and indirect infringement of the '846 Patent in an amount to be proved at trial.

59. LHD has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '846 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT V
(Infringement of the '421 Patent)

60. Paragraphs 1 through 19 are incorporated by reference as if fully set forth herein.

61. LHD has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '421 Patent.

62. Defendant has and continues to directly infringe the '421 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '421 Patent. Such products

include utilities, such as the Check Point Gateway and Firewall units that control network traffic by limiting and/or assigning processes and addresses. On information and belief, infringing products include at least the Gateway and Firewall products specified above as Accused Products.

63. For example, Defendant has and continues to directly infringe at least claim 90 of the '421 Patent by making, using, offering to sell, selling, and/or importing into the United States products that perform the method for restricting network address-based communication by selected processes to a set of specific network addresses. The Accused Products associate at least one selected process, such as, for example, HTTP or FTP, with at least one network address, such as, for example, a MAC address. The Accused Products detect when a selected process attempts to communicate via an unassociated address, such as when a process, such as HTTP, is disallowed for a specific address. The Accused Products then prevent the communication from proceeding.⁹

64. Defendant has and continues to indirectly infringe one or more claims of the '421 Patent by knowingly and intentionally inducing others, including Check Point customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology and by directing their customers to utilize the Accused Products in an infringing matter through marketing and support materials.¹⁰

65. Defendant, with knowledge that these products, or the use thereof, infringe the '421 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and

⁹ See, e.g., https://sc1.checkpoint.com/documents/R77.20.80/600_700_AdminGuide/html_frameset.htm?topic=documents/R77.20.80/600_700_AdminGuide/97593

¹⁰ See, *Id.*

continues to knowingly and intentionally induce, direct infringement of the '421 Patent by providing these products to end users for use in an infringing manner.

66. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the '421 Patent, but while remaining willfully blind to the infringement.

67. LHD has suffered damages as a result of Defendant's direct and indirect infringement of the '421 Patent in an amount to be proved at trial.

68. LHD has suffered, and will continue to suffer irreparable harm as a result of Defendant's infringement of the '421 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, LHD prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Patents-in-Suit;

c. An order awarding damages sufficient to compensate LHD for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding LHD its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e. Such other and further relief as the Court deems just and proper.

Dated: November 20, 2019

Respectfully submitted,

/s/ Alfred R. Fabricant

Alfred R. Fabricant
NY Bar No. 2219392
Email: afabricant@brownrudnick.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@brownrudnick.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@brownrudnick.com
BROWN RUDNICK LLP
7 Times Square
New York, NY 10036
Telephone: (212) 209-4800
Facsimile: (212) 209-4801

Justin Kurt Truelove
Texas Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston
Marshall, Texas 75670
Telephone: (903) 938-8321
Facsimile: (903) 215-8510

**ATTORNEYS FOR PLAINTIFF
LONGHORN HD LLC.**