



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/563,261	09/29/2017	Carlos Eduardo ORÉ	2210592.02089US5	8292
23483	7590	10/29/2018	EXAMINER	
WILMERHALE/BOSTON			PLECHA, THADDEUS J	
60 STATE STREET			ART UNIT	
BOSTON, MA 02109			PAPER NUMBER	
			2438	
			NOTIFICATION DATE	
			DELIVERY MODE	
			10/29/2018	
			ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

teresa.maia@wilmerhale.com
whipusptopairs@wilmerhale.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.
2. The following is a Non-Final Office Action in response to communications received on September 29, 2017. Claims 1-13 are pending and addressed below.

Specification

3. For the record, Examiner acknowledges the specification submitted on September 29, 2017 has been accepted.

Drawings

4. For the record, Examiner acknowledges the drawings submitted on September 29, 2017 have been accepted.

Claim Objections

5. Claims 1, 4 and 5 are objected to because of the following informalities:
 - a. The preamble of claim 1 recites a “multi-perimeter firewall”, however, the rest of the claim goes on to describe several system components that are not specifically part of a single firewall. It is suggested the limitation be amended to “multi-perimeter firewall system” for clarity and consistency. (Note: if the

preamble is amended in claim 1, the preamble in claims 2-13 should also be amended).

b. Claims 4 and 5 recite the limitation “the communication path” which lacks antecedent basis. It is suggested the limitations be amended to “~~the~~ a communication path” for clarity and consistency.

6. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 2 and 10 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

a. Claim 2 recites the limitation “the end access point servers.” There is insufficient antecedent basis for this limitation. Parent claim 1 previously recites “first” and “second” “access point servers” and also recites an “endpoint device” but never recites an “end access point server.” Therefore, it is unclear as to what end access point servers the limitation is referring.

b. Claim 10 recites the limitation “the traffic.” There are multiple previously recited traffic and it is unclear as to which particular traffic the limitation is referring.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 1-13 are rejected under 35 U.S.C. 101 because the claims fail to fall within one of the four statutory categories of invention. Claim 1 is directed towards a multi-perimeter firewall [system] comprising “an egress ingress point device”, “a first access point server”, “a second access point server”, “an endpoint device”, “a first firewall” and “a second firewall”. None of the claimed devices, servers or firewalls are specifically defines in the claims or in the instant specification as being hardware. As is known in the art, all of the claimed devices, servers and firewalls may be accomplished through software. Therefore, the claim is considered to be directed towards software per se and is therefore, non-statutory. Applicant may overcome this rejection by specifically defining one or more of the devices, servers and firewalls as hardware.

11. Dependent claims 2-13 are rejected for failing to further define parent claim 1 as statutory.

Claim Rejections - 35 USC § 103

12. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

13. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 1-3, 8 and 9 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida et al. (U.S. Pub. No. 2002/0046253 and hereinafter referred to as Uchida) in view of Feghali et al. (U.S. Pub. No. 2015/0128246 and hereinafter referred to as Feghali).

As to **claim 1**, Uchida discloses a multi-perimeter firewall in a global virtual network, comprising:

an egress ingress point device (**paragraphs [0005], [0006], [0047] and [0065]-[0067] and Figs. 1 and 3, Uchida teaches an internal server capable of sending and receiving data**);

a first access point server in communication with the egress ingress point device (**paragraphs [0005], [0006], [0048] and [0065] and Figs. 1 and 3, Uchida teaches a router connected to the internal server**);

a second access point server in communication with the first access point sever (**paragraphs [0049] and Figs. 1 and 3, Uchida teaches an external server connected to the router**);

an endpoint device in communication with the second access point server (**paragraphs [0049] and Figs. 1 and 3, Uchida teaches user computers connected to the external server**);

a first firewall in communication with the first access point server (**paragraphs [0005], [0006], [0048] and [0065] and Figs. 1 and 3, Uchida teaches the router contains firewall**); and

a second firewall in communication with the second access point server (**paragraphs [0015] and [0049] and Figs. 1 and 3, Uchida teaches the external server contains a second firewall.**). Uchida does not specifically disclose wherein the first firewall prevents at least some traffic from passing from the first access point server to the second access point server; and wherein the second firewall prevents at least some traffic from passing from the second access point server to the end point device as claimed. However, Feghali does disclose

wherein the first firewall prevents at least some traffic from passing from the first access point server to the second access point server; and wherein the second firewall prevents at least some traffic from passing from the second access point server to the end point device (**paragraphs [0029]-[0030] and Fig. 1, Feghali teaches multiple firewalls connected in series where each firewall controls data coming into and going out of a network.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the invention of Uchida with the teachings of Feghali for having the first and second firewalls prevent at least some traffic from passing because this would increase security.

As to **claim 2**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 1, wherein at least one of the end access point servers is configured to perform firewall services **(paragraphs [0049] and Figs. 1 and 3, Uchida teaches the external server contains a firewall.)**.

As to **claim 3**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 1, wherein the first firewall is in communication with the second firewall **(paragraphs [0048], [0049] and Figs. 1 and 3, Uchida teaches the two firewalls are communicatively coupled.)**.

As to **claim 8**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 1, wherein at least one of the firewalls performs deep packet inspection **(paragraph [0138], Feghali teaches deep packet inspection.)**.

Examiner supplies the same rationale for the combination of the references as in claim 1 above.

As to **claim 9**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 8, wherein the deep

packet inspection is performed on flow through traffic (**paragraph [0138],
Feghali teaches a firewall examining traffic traversing it.**).

Examiner supplies the same rationale for the combination of the references as in claim 1 above.

15. Claim 4 is rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claim 3 above, and further in view of Cicic et al. (U.S. Pub. No. 2010/0325309 cited in the IDS filed on 03/01/2018 and hereinafter referred to as Cicic).

As to **claim 4**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 3. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel as claimed. However, Cicic does disclose

wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel (**paragraphs [0060] and [0078] and Abstract, Cicic teaches a global virtual network with tunnels for communication.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Cicic for having a global virtual network tunnel because this would increase security and flexibility.

16. Claim 5 is rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claim 3 above, and further in view of Bhamidipati et al. (U.S. Pub. No. 2014/0210693 and hereinafter referred to as Bhamidipati).

As to **claim 5**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 3. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the communication path between the first firewall and the second firewall is a global virtual network back channel as claimed. However, Bhamidipati does disclose wherein the communication path between the first firewall and the second firewall is a global virtual network back channel (**paragraph [0007], Bhamidipati teaches a virtual network with back channel communications.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Bhamidipati for having a global virtual network back channel because this would increase security.

17. Claim 6 is rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claim 3 above, and further in view of Vissamsetty et al. (U.S. Pub. No. 2015/0326588 and hereinafter referred to as Vissamsetty).

As to **claim 6**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 3. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the first firewall and the second firewall share threat information including at least

one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors as claimed. However, Vissamsetty does disclose wherein the first firewall and the second firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors (**paragraphs [0132] and [0167], Vissamsetty teaches signatures are exported and shared among security devices.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Vissamsetty for sharing threat information because this would increase security.

18. Claim 7 is rejected under 35 U.S.C. 103 as being unpatentable over Uchida, Feghali and Vissamsetty as applied to claim 6 above, and further in view of Banfield et al. (U.S. Pub. No. 2015/0281176 and hereinafter referred to as Banfield).

As to **claim 7**, the combination of teachings between Uchida, Feghali and Vissamsetty disclose the multi-perimeter firewall according to claim 6. The combination of teachings between Uchida, Feghali and Vissamsetty does not specifically disclose wherein the first firewall and the second firewall share threat information with a central control server as claimed. However, Banfield does disclose

wherein the first firewall and the second firewall share threat information with a central control server (**paragraph [0016] and Abstract, Banfield teaches firewalls sharing traffic data with a central server.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Banfield for sharing threat information with a central control server because this would increase security.

19. Claim 10 is rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claim 8 above, and further in view of Tola (U.S. Pub. No. 2016/0337484).

As to **claim 10**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 8. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the deep packet inspection is performed on a cloned copy of the traffic as claimed. However, Tola does disclose

wherein the deep packet inspection is performed on a cloned copy of the traffic (**paragraphs [0050], [0183] and [0189], Tola teaches cloning traffic for security monitoring.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Tola for using a cloned copy of the traffic because

this would allow for security inspection without disrupting the traffic flow, thus improving performance and user experience.

20. Claims 11 and 12 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claim 1 above, and further in view of Staats et al. (U.S. Pub. No. 2005/0235352 and hereinafter referred to as Staats).

As to **claim 11**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 1. The combination of teachings between Uchida and Feghali does not specifically disclose wherein at least one of the firewalls performs stateful packet inspection as claimed.

However, Staats does disclose

wherein at least one of the firewalls performs stateful packet inspection
(paragraph [0033], Staats teaches performing stateful inspection.)

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Staats for performing stateful packet inspection because this would increase security.

As to **claim 12**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 1. The combination of teachings between Uchida and Feghali does not specifically disclose wherein one firewall performs stateful packet inspection and the other firewall performs stateful packet inspection as claimed. However, Staats does disclose

wherein one firewall performs stateful packet inspection and the other firewall performs stateful packet inspection (**paragraph [0033], Staats teaches performing stateful inspection.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Staats for performing stateful packet inspection because this would increase security.

21. Claim 13 is rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claim 1 above, and further in view of Shieh (U.S. Pub. No. 2012/0210417).

As to **claim 13**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall according to claim 1. The combination of teachings between Uchida and Feghali does not specifically disclose wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand as claimed. However, Shieh does disclose

wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand (**paragraph [0034], Shieh teaches dynamically load balancing on a cloud that has firewalls.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of

Uchida with the teachings of Shieh for having a cloud firewall load balancer because this would increase efficiency.

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THADDEUS J PLECHA whose telephone number is (571)270-7506. The examiner can normally be reached on M-F 8-4:30.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THADDEUS J PLECHA/
Examiner, Art Unit 2438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Carlos Eduardo Oré et al. Confirmation No.: 8292
Application No.: 15/563,261 Art Unit: 2438
Filed: September 29, 2017 Examiner: T. J. Plecha
Title: MULTI-PERIMETER FIREWALL IN THE CLOUD

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.111

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Office Action dated October 29, 2018, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 6 of this paper.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently amended) A multi-perimeter firewall system located in a cloud and forming part of ~~[[in]]~~ a global virtual network, comprising:
 - an egress ingress point device;
 - a first access point server in communication with the egress ingress point device;
 - a second access point server in communication with the first access point sever;
 - an endpoint device in communication with the second access point server;
 - a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server; and
 - a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device.
2. (Currently amended) The multi-perimeter firewall system according to claim 1, wherein at least one of the ~~[[end]]~~access point servers is configured to perform firewall services.
3. (Currently amended) The multi-perimeter firewall system according to claim 1, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path.
4. (Currently amended) The multi-perimeter firewall system according to claim 3, wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel.
5. (Currently amended) The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a global virtual network back channel.

6. (Currently amended) The multi-perimeter firewall system according to claim 3, wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.
7. (Currently amended) The multi-perimeter firewall system according to claim 6, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.
8. (Currently amended) The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls performs deep packet inspection.
9. (Currently amended) The multi-perimeter firewall system according to claim 8, wherein the deep packet inspection is performed on flow through traffic.
10. (Currently amended) The multi-perimeter firewall system according to claim 8, wherein the deep packet inspection is performed on a cloned copy of [[the]]traffic that flows through the at least one of the first perimeter firewall and the second perimeter firewall.
11. (Currently amended) The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls performs stateful packet inspection.
12. (Currently amended) The multi-perimeter firewall system according to claim 1, wherein one firewall performs stateful packet inspection and the other firewall performs ~~stateful~~ deep packet inspection.
13. (Currently amended) The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.

14. (New) A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:
- an egress ingress point device;
 - a first access point server in communication with the egress ingress point device;
 - a second access point server in communication with the first access point sever;
 - an endpoint device in communication with the second access point server;
 - a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server using a first firewall mechanism; and
 - a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device using a second, different firewall mechanism.
15. (New) The multi-perimeter firewall system according to claim 14, wherein at least one of the access point servers is configured to perform firewall services.
16. (New) The multi-perimeter firewall system according to claim 14, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path.
17. (New) The multi-perimeter firewall system according to claim 16, wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel.
18. (New) The multi-perimeter firewall system according to claim 16, wherein the communication path between the first perimeter firewall and the second perimeter_firewall is a global virtual network back channel.
19. (New) The multi-perimeter firewall system according to claim 16, wherein the first perimeter firewall and the second perimeter_firewall share threat information including at least one

of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.

20. (New) The multi-perimeter firewall system according to claim 19, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.

21. (New) The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls performs deep packet inspection.

22. (New) The multi-perimeter firewall system according to claim 21, wherein the deep packet inspection is performed on flow through traffic.

23. (New) The multi-perimeter firewall system according to claim 21, wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the at least one of the first perimeter firewall and the second perimeter firewall.

24. (New) The multi-perimeter firewall system according to claim 14, wherein at least one of the firewalls performs stateful packet inspection.

25. (New) The multi-perimeter firewall system according to claim 14, wherein one firewall performs stateful packet inspection and the other firewall performs deep packet inspection.

26. (New) The multi-perimeter firewall system according to claim 14, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.

27. (New) The multi-perimeter firewall system according to claim 14, wherein the second perimeter firewall is between the endpoint device and the second access point server.

28. (New) The multi-perimeter firewall system according to claim 14, wherein the first perimeter firewall is between the first access point server and the second access point server.

REMARKS

I. Status of the Claims

Claims 1-13 were pending in the present application (the “Application”) prior to the amendments submitted herein. In this response, claims 1-13 have been amended. Claims 14-28 have been added. Support for the new claims is found throughout the Application, including at least ¶¶ 107, 114-115, 126, 130-131 and Figure 12 of the Application. No new matter has been added. Upon entry of the amendment, claims 1-28 will be pending. Applicant respectfully requests reconsideration and allowance of the Application in view of the claim amendments and the following comments.

II. Claim Objections

Claims 1, 4, and 5 have been objected to because of informalities. Office Action at 2-3. Applicant submits that the amendments overcome these objections.

III. Claim Rejections - 35 U.S.C. § 112

Claims 2 and 10 have been rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, as allegedly being indefinite. Office Action at 3-4. In particular, the Office Action alleges that the limitation “the end access point servers” recited in claim 2 lacks antecedent basis. *Id.* at 3. Applicant has amended claim 2 by replacing the limitation “the end access point servers” with “the access point servers.” Applicant submits that the amendment overcomes this rejection.

The Office Action further alleges that the limitation “the traffic” recited in claim 10 is indefinite because “it is unclear as to which particular traffic the limitation is referring.” Office Action at 3. Applicant has amended claim 10 by replacing the limitation “the traffic” with “traffic that flows through the at least one of the first perimeter firewall and the second perimeter firewall.” Applicant submits the amendment overcomes this rejection.

In view of the foregoing, Applicant respectfully requests that the Examiner reconsider and withdraw these grounds of rejection.

IV. Claim Rejections - 35 U.S.C. § 101

Claims 1-13 have been rejected under 35 U.S.C. § 101 as allegedly being directed towards software per se. Office Action at 4. Applicant respectfully disagrees.

On January 7, 2019, the USPTO published its 2019 Revised Patent Subject Matter Eligibility Guidance (“2019 Revised Guidance”). The 2019 Revised Guidance specifies that, except in “rare circumstances,” a claim must recite one of three enumerated categories to recite an “abstract idea,” namely, (1) mathematical concepts, (2) methods of organizing human activity, or (3) mental processes. 2019 Revised Guidance at 9-11. The Office Action alleges generally that claim 1 is “directed towards software per se.” Office Action at 4. The Office Action, however, fails to identify which limitation or limitations, if any, allegedly recite one of the three categories explicitly enumerated in the 2019 Revised Guidance. Further, software-based claims are not inherently abstract, so even if a claim were directed to software per se, that would not make it patent ineligible. 2019 Revised Guidance at FN 11 (quoting *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016) (“claims directed to software” are not “inherently abstract.”).) Thus, the Office Action has not established that claim 1 recites an abstract idea. Accordingly, Applicant respectfully requests the rejection be withdrawn.

Under the 2019 Revised Guidance, even if a claim recites an abstract idea, “[a] claim is not ‘directed to’ a judicial exception, and thus is patent eligible, if the claim as a whole integrates the recited judicial exception into a practical application of that exception.” 2019 Revised Guidance at 13-14. Further, if “an additional element reflects an improvement in the functioning of a computer, or an improvement to other technology or technical field,” then it is “indicative that [the] additional element (or combination of elements) may have integrated the exception into a practical application.” *Id.* at 19.

Even if claim 1 were directed to an abstract idea—which it is not—it is a practical application and is therefore patent eligible. Claim 1 as amended is related to a multi-perimeter firewall system that employs at least two perimeter firewalls that prevent some traffic from passing among different locations. According to the configuration of claim 1, packets rejected by one of the first and second perimeter firewalls do not make it through the global virtual network to the other of the first and second perimeter firewall, meaning that the amount of packets that need to be scanned by each

individual firewall can be reduced. This can correspondingly reduce the computational resources required to implement each individual perimeter firewall. Thus, claim 1 as amended recites an improvement in the technical area of the firewall system. Accordingly, even assuming for the sake of argument that claim 1 recites one of the enumerated categories of abstract ideas, which it does not, claim 1 as amended is not directed to an abstract idea because any alleged abstract idea is “integrated into a practical application.” In this case, that practical application is a firewall system with an improvement for the computational resources required to implement each individual perimeter firewall.

Moreover, even if claim 1 were directed to an abstract idea – which it is not – it would still be patent eligible because it recites an inventive concept that amounts to significantly more than an abstract idea. Under the 2019 Revised Guidance, it is “indicative that an inventive concept may be present” if a claim adds “a specific limitation or combination of limitations that are not well-understood, routine, conventional activity in the field.” 2019 Revised Guidance at 23; *see also Berkheimer v. HP Inc.*, 881 F.3d 1360 (Fed. Cir. 2018); USPTO Memorandum of April 19, 2018, “Changes in Examination Procedure Pertaining to Subject Matter eligibility, recent Subject Matter Eligibility Decision (*Berkheimer v. HP, Inc.*)” (April 19, 2018).

The Office Action does not cite any authority, as required by *Berkheimer*, to support that any of the specific additional elements as recited in claim 1 are well-understood. As discussed below, the cited prior art references, either alone or in combination, fail to teach or suggest all limitations of claim 1. Claim 1 thus recites additional features that are **not** well-understood, routine, or conventional. Accordingly, claim 1 recites significantly more than an abstract idea.

In summary, claim 1 as amended is directed to patent eligible subject matter. Claims 2-13 depend, directly or indirectly, from claim 1 and are directed to patent eligible subject matter at least by virtue of their dependency from claim 1.

V. Claim Rejections - 35 U.S.C. § 103

The Examiner has rejected claims 1-3, 8, and 9 under 35 U.S.C. § 103 as allegedly being unpatentable over U.S. Publication No. 2002/0046253 to Uchida et al. (“Uchida”) in view of U.S. Publication No. 2015/0128246 to Feghali et al. (“Feghali”); claim 4 under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S.

Publication No. 2010/0325309 to Cicic et al. (“Cicic”); claim 5 under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2014/0210693 Bhamidipati et al. (“Bhamidipati”); claim 6 under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2015/0326588 to Vissamsetty et al. (“Vissamsetty”); claim 7 under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of (U.S. Publication No. 2015/0281176 to Banfield et al. (“Banfield”); claim 10 under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2016/0337484 to Tola (“Tola”); claims 11 and 12 under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2005/0235352 to Staats et al. (“Staats”); and claim 13 under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2012/0210417 to Shieh (“Shieh”). Office Action at 5-14. Applicant respectfully disagree.

Independent claim 1, as amended, recites, in part, the following limitations: “a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server;” and “a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device.”

As explained in Section IV, *supra*, claim 1 as amended is related to a multi-perimeter firewall system that employs at least two perimeter firewalls that prevent some traffic from passing among different locations. According to the configuration of claim 1, packets rejected by one of the first and second perimeter firewalls do not make it through the global virtual network to the other of the first and second perimeter firewall, meaning that the amount of packets that need to be scanned by each individual firewall can be reduced. This can correspondingly reduce the computational resources required to implement each individual perimeter firewall.

The Office Action acknowledges that Uchida does not teach the limitations discussed above, *i.e.*, “a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the

second access point server using a first firewall mechanism;” and “a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device using a second, different firewall mechanism.” Office Action at 6. Applicant agrees.

The Office Action cites Feghali (at ¶¶29-30 and Fig. 1) as allegedly disclosing the following limitations that were recited in original claim 1: “a first firewall in communication with the first access point server, wherein the first firewall prevents at least some traffic from passing from the first access point server to the second access point server;” and “a second firewall in communication with the second access point server, wherein the second firewall prevents at least some traffic from passing from the second access point server to the end point device.” Office Action at 6. Applicant respectfully disagrees.

Feghali discloses a system “for protecting a network against malicious attacks or attempts for unauthorized access.” Feghali at Abstract. The cited portions of Feghali disclose, at best, that multiple firewalls can be connected in series. *Id.* at ¶30. Those firewalls, however, are all located between two components. For example, in Figure 1 (reproduced below) of Feghali, all firewalls 150 are located between the corporate network/LAN 110 and the Internet/WAN 160. Therefore, the firewalls disclosed in Feghali can at best prevent some traffic from passing between a first component (*e.g.*, the corporate network/LAN 110) and a second component (*e.g.*, the Internet/WAN 160).

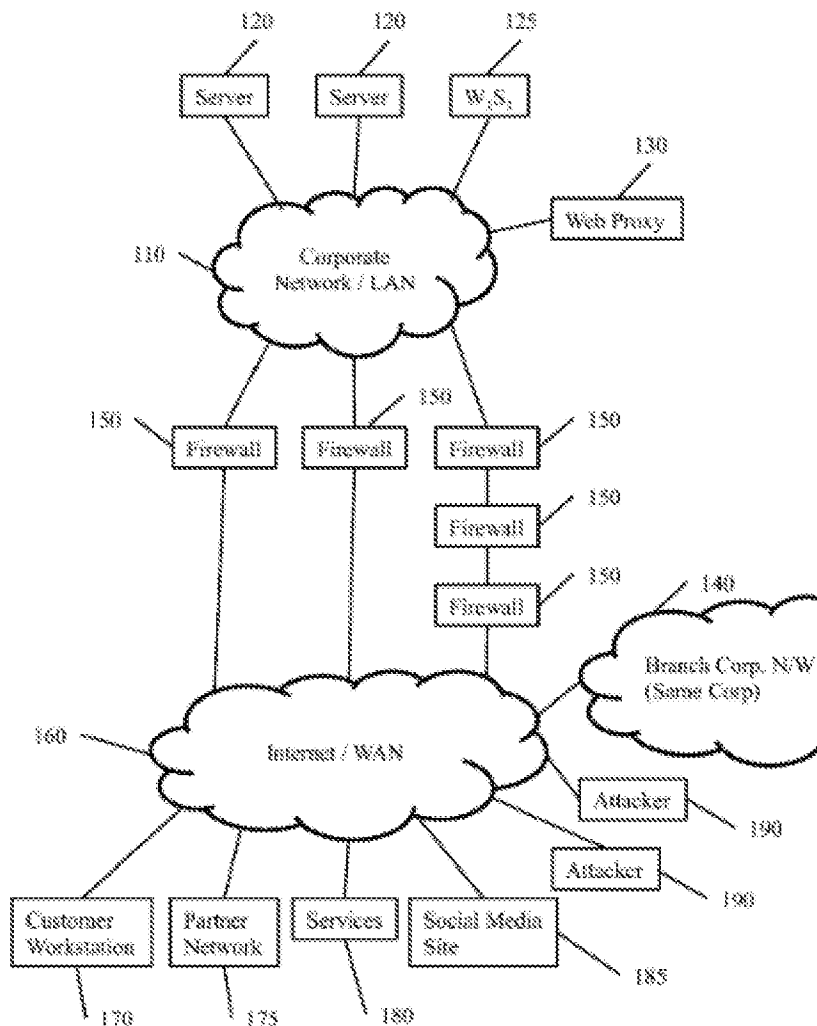


Figure 1 (Prior Art)

In contrast to Feghali, claim 1 as amended requires that “the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server” and “the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device.” Therefore, the firewalls in claim 1 prevent some traffic that is associated with at least *three* components – the first access point server, the second access point server, and the end point device. Because the firewalls disclosed in Feghali can at best prevent some traffic from passing between *two* components, Feghali fails to disclose the following limitations of claim 1: “a first perimeter firewall in communication with the first access

point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server;” and “a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device.”

Because neither Uchida nor Feghali, nor the combination of Uchida and Feghali, discloses every limitation from claim 1 as amended, claim 1 is not obvious over the combination of Uchida and Feghali. Accordingly, Applicant respectfully submits that claim 1 is patentable over Uchida and Feghali, and Applicant requests withdrawal of the Examiner’s obviousness rejections.

The Office Action does not rely on Cicic, Bhamidipati, Vissamsetty, Banfield, Tola, Staats, or Shieh as disclosing the limitations recited above for independent claim 1 as amended – including, for example, that “a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server” and “a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device.” Applicant further submits that the cited portions of these references do not disclose the features of independent claim 1. Therefore, claim 1 is patentable over the combination of Uchida, Feghali, and these other cited references.

Further, claims 2-13 depend directly or indirectly from independent claim 1. Therefore, for at least the reasons provided above with respect to claim 1, these dependent claims are patentable over the cited references.

In view of the foregoing, Applicant respectfully requests that the Examiner reconsider and withdraw this ground of rejection.

VI. New Claims

Applicant has added new claims 14-28 to more fully claim the invention. Support for the new claims is found throughout the Application, including at least ¶¶107, 114-115, 126, 130-131 and Figure 12 of the Application. No new matter has been added. Applicant submits that none of the cited references discloses the features of claims 14-28.

VII. Conclusion

In view of the above amendment, Applicant believes the pending application is in condition for allowance.

In the event the U.S. Patent and Trademark Office determines that an extension is required, Applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 08-0219 referencing docket no. 2210592.02089US5.

Respectfully submitted,

Dated: January 28, 2019

/Yu Yang/
Yu Yang
Registration No.: 68,839
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/563,261	09/29/2017	Carlos Eduardo ORÉ	2210592.02089US5	8292
23483	7590	03/22/2019	EXAMINER	
WILMERHALE/BOSTON			PLECHA, THADDEUS J	
60 STATE STREET			ART UNIT	
BOSTON, MA 02109			PAPER NUMBER	
			2438	
			NOTIFICATION DATE	
			DELIVERY MODE	
			03/22/2019	
			ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

teresa.maia@wilmerhale.com
whipusptopairs@wilmerhale.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.
2. The following is a Final Office Action in response to communications received on January 28, 2019. Claims 1-13 have been amended. No claims have been newly cancelled. Claims 14-28 have been newly added. Therefore, claims 1-28 are pending and addressed below.

Response to Arguments

4. Applicant's amendments are sufficient to overcome the claim objections for claims 1, 4 and 5 set forth in the previous Office Action.
5. Applicant's amendments are sufficient to overcome the 35 U.S.C. 112(b) rejections for claims 2 and 10 set forth in the previous Office Action.
6. Applicant's arguments regarding the rejections under 35 U.S.C. 101 have been fully considered but are not persuasive. Applicant argues:
 - i) The claims are not directed towards an abstract idea (pp. 7-8 of Remarks).
7. Applicant's arguments regarding the rejections under 35 U.S.C. 103 have been fully considered but are not persuasive. Applicant argues:

ii) Uchida and Feghali do not disclose or suggest “a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server” and “a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device” (pp. 9-12 of Remarks).

8. In response to Applicant’s arguments:

i) Applicant is arguing that the claims are not directed towards an abstract idea. Applicant makes several arguments regarding how the claims are not directed towards an abstract idea and even if they were, there is significantly more recited in the claims based on the Office guidance. Examiner respectfully disagrees inasmuch as Examiner never stated that the claims were rejected under 101 as being directed towards abstract ideas. Examiner stated very clearly in the previous Office Action that the claims are rejected under 101 for being directed towards software per se. It has long been held that claims directed towards “software per se” do not fall within one of the four statutory categories of invention (see also MPEP 2106.03 I – “Non-limiting examples of claims that are not directed to any of the statutory categories include: Products that do not have a physical or tangible form, such as information (often referred to as ‘data per se’) or **a computer program per se (often referred to as ‘software per se’)** when claimed as a product without any structural recitations” – emphasis added). Applicant has not amended the claims to specifically add a piece of

hardware into the body of the claims. Since Applicant's argument is not pertinent to the rejection at hand, Applicant's argument is not persuasive and the rejection is maintained and repeated herein below.

ii) Applicant is arguing that Uchida and Feghali do not disclose or suggest "a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server" and "a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device." Applicant's arguments concentrate on the Feghali reference. Applicant specifically argues that Feghali at best discloses multiple firewalls can be connected in series but that those firewalls are connected between two components. Applicant argues that the claims require preventing traffic between "**three** components" and that Feghali can only prevent traffic between "**two** components" (emphasis added by Applicant). Applicant then concludes that Feghali does not teach the cited claimed limitations. Examiner respectfully disagrees for at least several reasons.

Initially, Applicant has made a statement that "The Office Action acknowledges that Uchida does not teach the limitations discussed above, *i.e.*, 'a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server' and 'a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device'."

This is a mischaracterization of the previous Office Action. Examiner made clear in the previous Office Action that Uchida does disclose “first *perimeter* firewall in communication with the first access point server” and “a second *perimeter* firewall in communication with the second access point server” (emphasis added on “perimeter” as this was added by Applicant after the previous Office Action). Examiner stated that the only portions of claim 1, for example, that Uchida did not disclose were “wherein the first *perimeter* firewall prevents at least some traffic from passing from the first access point server to the second access point server” and “wherein the second *perimeter* firewall prevents at least some traffic from passing from the second access point server to the end point device” (emphasis added on “perimeter” as this was added by Applicant after the previous Office Action). This is an important distinction as Uchida does very clearly show two different firewalls in between different components. Fig. 1 of Uchida very clearly discloses a first firewall (FW on device 35) between several components and a second firewall (FW on device 23) located between several components. Thus, it is clear from Uchida that firewalls are placed alternately between devices. Therefore, Applicant’s arguments are not persuasive.

Additionally, even though Examiner contends that the prior art discloses Applicant’s interpretation of the claim language as stated above, Examiner further contends that Applicant is providing only a very narrow interpretation of the claim language and Applicant’s claims actually allow for a broader interpretation. For example, even though Applicant’s claims may be interpreted as having two firewalls located between three devices as argued by Applicant (i.e. a first firewall between a first access point server and a second access point server and a second firewall between

the second access point server and an end point device), Applicant's claims never actually require this exact setup. The claims require, *inter alia*, two firewalls and for the first firewall to prevent some traffic from passing from a first access point server to a second access point server and for the second firewall to prevent some traffic from passing from the second access point server to an end point device. Additionally the claims require, *inter alia*, that the first firewall be "in communication with" the first access point server and the second firewall be "in communication with" the second access point server. The phrase "in communication with" does not provide an exact location of where the firewalls are in relation the access point servers. For a first firewall to be "in communication with" a first access point server, the first firewall would only need to be connected in some way (directly or indirectly through several devices in-between) that allowed communication between itself and the first access point server. Therefore, interpretations of the claims where there are several devices between the access point servers and the firewalls or where the firewalls are located on the access point servers themselves are all possible interpretations of the claim language under a broadest reasonable interpretation guideline. Thus, even if, *arguendo*, Applicant's interpretation of the prior art were correct and Feghali only taught two firewalls in series between only two components (which Examiner does not concede to), Feghali could still read on the claim language as the firewalls in Feghali would still be "in communication with" three devices. Moreover, a firewall that is placed before (in the sense of traffic flow) a first access point server would be able to be "in communication with" the first access point server and prevent some traffic from passing from the first access point server to a second access point server downstream of the first access point server. This is because

the firewall would prevent the traffic from ever arriving at the first access point server, thus preventing the traffic from passing from the first access point server to the second access point server. A similar argument can be made for preventing traffic from passing from the second access point server to an end point device. A reference where two firewalls are both placed in series before a first access point server with no devices in between them could also read on the claim language in the scenario described above. There are obviously other variations that would also read on Applicant's claim language. Therefore, Applicant's claim language is broader than Applicant's interpretation, Applicant is arguing features that are not limited by the claim, and Applicant's arguments are not persuasive.

Examiner's Note

9. Applicant is advised that should claims 8-10 be found allowable, claims 21-23 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim.

See MPEP § 706.03(k).

Claim Objections

10. Claims 21-23 objected to because of the following informalities: Claims 21-23 are duplicate claims of claims 8-10. It appears as though the dependency of claim 21

was meant to be on claim 14 and not claim 1. It is suggested the dependency of claim 21 be changed to 14 so as to no longer be a duplicate claim.

11. Appropriate correction is required.

Claim Rejections - 35 USC § 101

12. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claims 1-28 are rejected under 35 U.S.C. 101 because the claims fail to fall within one of the four statutory categories of invention. Claim 1 is directed towards a multi-perimeter firewall system comprising “an egress ingress point device”, “a first access point server”, “a second access point server”, “an endpoint device”, “a first perimeter firewall” and “a second perimeter firewall”. None of the claimed devices, servers or firewalls are specifically defined in the claims or in the instant specification as being hardware. As is known in the art, all of the claimed devices, servers and firewalls may be accomplished through software. Therefore, the claim is considered to be directed towards software per se and is therefore, non-statutory. Applicant may overcome this rejection by specifically defining one or more of the devices, servers and firewalls as hardware. Claim 14 is rejected for similar reasons to claim 1.

14. Dependent claims 2-13 and 15-28 are rejected for failing to further define parent claims 1 and 14 as statutory.

Claim Rejections - 35 USC § 103

15. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

16. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

17. Claims 1-3, 8, 9, 14-16, 21 and 22 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida et al. (U.S. Pub. No. 2002/0046253 and hereinafter referred to as Uchida) in view of Feghali et al. (U.S. Pub. No. 2015/0128246 and hereinafter referred to as Feghali).

As to **claim 1**, Uchida discloses a multi-perimeter firewall system, comprising:

an egress ingress point device (**paragraphs [0005], [0006], [0047] and [0065]-[0067] and Figs. 1 and 3, Uchida teaches an internal server capable of sending and receiving data**);

a first access point server in communication with the egress ingress point device (**paragraphs [0005], [0006], [0048] and [0065] and Figs. 1 and 3, Uchida teaches a router connected to the internal server**);

a second access point server in communication with the first access point sever (**paragraphs [0049] and Figs. 1 and 3, Uchida teaches an external server connected to the router**);

an endpoint device in communication with the second access point server (**paragraphs [0049] and Figs. 1 and 3, Uchida teaches user computers connected to the external server**);

a first perimeter firewall in communication with the first access point server (**paragraphs [0005], [0006], [0048] and [0065] and Figs. 1 and 3, Uchida teaches the router contains firewall**); and

a second perimeter firewall in communication with the second access point server (**paragraphs [0015] and [0049] and Figs. 1 and 3, Uchida teaches the external server contains a second firewall.**). Uchida does not specifically disclose located in a cloud and forming part of a global virtual network; wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server; and wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device as claimed. However, Feghali does disclose

located in a cloud and forming part of a global virtual network (**paragraphs [0026], [0027], [0039] and [0193], Feghali teaches a virtual network with cloud computing**);

wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server; and

wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device **(paragraphs [0029]-[0030] and Fig. 1, Feghali teaches multiple firewalls connected in series where each firewall controls data coming into and going out of a network.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the invention of Uchida with the teachings of Feghali for having the first and second firewalls prevent at least some traffic from passing because this would increase security.

As to **claim 2**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 1, wherein at least one of the access point servers is configured to perform firewall services **(paragraphs [0049] and Figs. 1 and 3, Uchida teaches the external server contains a firewall.)**.

As to **claim 3**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 1, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path **(paragraphs [0048], [0049] and Figs. 1 and 3, Uchida teaches the two firewalls are communicatively coupled.)**.

As to **claim 8**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls performs deep packet inspection **(paragraph [0138], Feghali teaches deep packet inspection.)**.

Examiner supplies the same rationale for the combination of the references as in claim 1 above.

As to **claim 9**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 8, wherein the deep packet inspection is performed on flow through traffic (**paragraph [0138], Feghali teaches a firewall examining traffic traversing it.**).

Examiner supplies the same rationale for the combination of the references as in claim 1 above.

As to **claim 21**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls performs deep packet inspection (**paragraph [0138], Feghali teaches deep packet inspection.**).

Examiner supplies the same rationale for the combination of the references as in claim 1 above.

As to **claim 22**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 21, wherein the deep packet inspection is performed on flow through traffic (**paragraph [0138], Feghali teaches a firewall examining traffic traversing it.**).

Examiner supplies the same rationale for the combination of the references as in claim 1 above.

As to **claim 14**, Uchida discloses a multi-perimeter firewall system, comprising:

an egress ingress point device (**paragraphs [0005], [0006], [0047] and [0065]-[0067] and Figs. 1 and 3, Uchida teaches an internal server capable of sending and receiving data**);

a first access point server in communication with the egress ingress point device (**paragraphs [0005], [0006], [0048] and [0065] and Figs. 1 and 3, Uchida teaches a router connected to the internal server**);

a second access point server in communication with the first access point sever (**paragraphs [0049] and Figs. 1 and 3, Uchida teaches an external server connected to the router**);

an endpoint device in communication with the second access point server (**paragraphs [0049] and Figs. 1 and 3, Uchida teaches user computers connected to the external server**);

a first perimeter firewall in communication with the first access point server (**paragraphs [0005], [0006], [0048] and [0065] and Figs. 1 and 3, Uchida teaches the router contains firewall**); and

a second perimeter firewall in communication with the second access point server (**paragraphs [0015] and [0049] and Figs. 1 and 3, Uchida teaches the external server contains a second firewall.**). Uchida does not specifically disclose located in a cloud and forming part of a global virtual network; wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server using a first firewall mechanism; and wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device

using a second, different firewall mechanism as claimed. However, Feghali does disclose

located in a cloud and forming part of a global virtual network

(paragraphs [0026], [0027], [0039] and [0193], Feghali teaches a virtual network with cloud computing);

wherein the first perimeter firewall prevents at least some traffic from passing from the first access point server to the second access point server using a first firewall mechanism; and wherein the second perimeter firewall prevents at least some traffic from passing from the second access point server to the end point device using a second, different firewall mechanism

(paragraphs [0029]-[0030] and Fig. 1, Feghali teaches multiple firewalls connected in series where each firewall controls data coming into and going out of a network and each firewall may be from different suppliers having different rules (i.e. different mechanisms).).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the invention of Uchida with the teachings of Feghali for having the first and second firewalls prevent at least some traffic from passing because this would increase security.

As to **claim 15**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 14, wherein at least one of the access point servers is configured to perform firewall services **(paragraphs [0049] and Figs. 1 and 3, Uchida teaches the external server contains a firewall.).**

As to **claim 16**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 14, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path (**paragraphs [0048], [0049] and Figs. 1 and 3, Uchida teaches the two firewalls are communicatively coupled.**).

18. Claims 4 and 17 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claims 3 and 16 above, and further in view of Cicic et al. (U.S. Pub. No. 2010/0325309 cited in the IDS filed on 03/01/2018 and hereinafter referred to as Cicic).

As to **claim 4**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 3. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel as claimed. However, Cicic does disclose

wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel (**paragraphs [0060] and [0078] and Abstract, Cicic teaches a global virtual network with tunnels for communication.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of

Uchida with the teachings of Cicic for having a global virtual network tunnel because this would increase security and flexibility.

As to **claim 17**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 16. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel as claimed. However, Cicic does disclose

wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel (**paragraphs [0060] and [0078] and Abstract, Cicic teaches a global virtual network with tunnels for communication.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Cicic for having a global virtual network tunnel because this would increase security and flexibility.

19. Claims 5 and 18 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claims 3 and 16 above, and further in view of Bhamidipati et al. (U.S. Pub. No. 2014/0210693 and hereinafter referred to as Bhamidipati).

As to **claim 5**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 3. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the communication path between the first perimeter firewall and the second perimeter firewall is a global virtual network back channel as claimed. However, Bhamidipati does disclose

wherein the communication path between the first perimeter firewall and the second perimeter firewall is a global virtual network back channel (**paragraph [0007], Bhamidipati teaches a virtual network with back channel communications.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Bhamidipati for having a global virtual network back channel because this would increase security.

As to **claim 18**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 16. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the communication path between the first perimeter firewall and the second perimeter firewall is a global virtual network back channel as claimed. However, Bhamidipati does disclose

wherein the communication path between the first perimeter firewall and the second perimeter firewall is a global virtual network back channel (**paragraph**

[0007], Bhamidipati teaches a virtual network with back channel communications.).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Bhamidipati for having a global virtual network back channel because this would increase security.

20. Claims 6 and 19 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claims 3 and 16 above, and further in view of Vissamsetty et al. (U.S. Pub. No. 2015/0326588 and hereinafter referred to as Vissamsetty).

As to **claim 6**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 3. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors as claimed. However, Vissamsetty does disclose

wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors (**paragraphs [0132] and [0167], Vissamsetty teaches signatures are exported and shared among security devices.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Vissamsetty for sharing threat information because this would increase security.

As to **claim 19**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 16. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors as claimed. However, Vissamsetty does disclose

wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors **(paragraphs [0132] and [0167], Vissamsetty teaches signatures are exported and shared among security devices.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Vissamsetty for sharing threat information because this would increase security.

21. Claims 7 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida, Feghali and Vissamsetty as applied to claims 6 and 19 above, and further in view of Banfield et al. (U.S. Pub. No. 2015/0281176 and hereinafter referred to as Banfield).

As to **claim 7**, the combination of teachings between Uchida, Feghali and Vissamsetty disclose the multi-perimeter firewall system according to claim 6. The combination of teachings between Uchida, Feghali and Vissamsetty does not specifically disclose wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server as claimed. However, Banfield does disclose

wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server (**paragraph [0016] and Abstract, Banfield teaches firewalls sharing traffic data with a central server.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Banfield for sharing threat information with a central control server because this would increase security.

As to **claim 20**, the combination of teachings between Uchida, Feghali and Vissamsetty disclose the multi-perimeter firewall system according to claim 19. The combination of teachings between Uchida, Feghali and Vissamsetty does not specifically disclose wherein the first perimeter firewall and the second

perimeter firewall share threat information with a central control server as claimed. However, Banfield does disclose

wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server (**paragraph [0016] and Abstract, Banfield teaches firewalls sharing traffic data with a central server.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Banfield for sharing threat information with a central control server because this would increase security.

22. Claims 10 and 23 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claims 8 and 21 above, and further in view of Tola (U.S. Pub. No. 2016/0337484).

As to **claim 10**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 8. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the at least one of the first perimeter firewall and the second perimeter firewall as claimed. However, Tola does disclose

wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the at least one of the first perimeter firewall and the second perimeter firewall (**paragraphs [0050], [0183] and [0189], Tola teaches cloning traffic for security monitoring.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Tola for using a cloned copy of the traffic because this would allow for security inspection without disrupting the traffic flow, thus improving performance and user experience.

As to **claim 23**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 21. The combination of teachings between Uchida and Feghali does not specifically disclose wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the at least one of the first perimeter firewall and the second perimeter firewall as claimed. However, Tola does disclose

wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the at least one of the first perimeter firewall and the second perimeter firewall (**paragraphs [0050], [0183] and [0189], Tola teaches cloning traffic for security monitoring.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Tola for using a cloned copy of the traffic because this would allow for security inspection without disrupting the traffic flow, thus improving performance and user experience.

23. Claims 11, 12, 24 and 25 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claims 1 and 14 above, and further

in view of Staats et al. (U.S. Pub. No. 2005/0235352 and hereinafter referred to as Staats).

As to **claim 11**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 1. The combination of teachings between Uchida and Feghali does not specifically disclose wherein at least one of the firewalls performs stateful packet inspection as claimed. However, Staats does disclose

wherein at least one of the firewalls performs stateful packet inspection **(paragraph [0033], Staats teaches performing stateful inspection.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Staats for performing stateful packet inspection because this would increase security.

As to **claim 12**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 1, and the other firewall performs deep packet inspection **(paragraph [0138], Feghali teaches deep packet inspection.)**. The combination of teachings between Uchida and Feghali does not specifically disclose wherein one firewall performs stateful packet inspection as claimed. However, Staats does disclose

wherein one firewall performs stateful packet inspection **(paragraph [0033], Staats teaches performing stateful inspection.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of

Uchida with the teachings of Staats for performing stateful packet inspection because this would increase security.

As to **claim 24**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 14. The combination of teachings between Uchida and Feghali does not specifically disclose wherein at least one of the firewalls performs stateful packet inspection as claimed. However, Staats does disclose

wherein at least one of the firewalls performs stateful packet inspection **(paragraph [0033], Staats teaches performing stateful inspection.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Staats for performing stateful packet inspection because this would increase security.

As to **claim 25**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 14, and the other firewall performs deep packet inspection **(paragraph [0138], Feghali teaches deep packet inspection.)**. The combination of teachings between Uchida and Feghali does not specifically disclose wherein one firewall performs stateful packet inspection as claimed. However, Staats does disclose

wherein one firewall performs stateful packet inspection **(paragraph [0033], Staats teaches performing stateful inspection.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Staats for performing stateful packet inspection because this would increase security.

24. Claims 13 and 26 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claims 1 and 14 above, and further in view of Shieh (U.S. Pub. No. 2012/0210417).

As to **claim 13**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 1. The combination of teachings between Uchida and Feghali does not specifically disclose wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand as claimed. However, Shieh does disclose

wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand (**paragraph [0034], Shieh teaches dynamically load balancing on a cloud that has firewalls.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Shieh for having a cloud firewall load balancer because this would increase efficiency.

As to **claim 26**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 14. The combination of teachings between Uchida and Feghali does not specifically disclose wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand as claimed. However, Shieh does disclose

wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand (**paragraph [0034], Shieh teaches dynamically load balancing on a cloud that has firewalls.**).

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Shieh for having a cloud firewall load balancer because this would increase efficiency.

25. Claims 27 and 28 are rejected under 35 U.S.C. 103 as being unpatentable over Uchida and Feghali as applied to claim 14 above, and further in view of Dosa Racz et al. (U.S. Pub. No. 2008/0010676 and hereinafter referred to as Dosa Racz).

As to **claim 27**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 14. While the combination of teachings between Uchida and Feghali does disclose two firewalls in between devices (see for example Figs. 1 and 3 of Uchida and Fig. 1 of Feghali), the combination of teachings between Uchida and Feghali is not

explicitly clear on disclosing wherein the second perimeter firewall is between the endpoint device and the second access point server as claimed. However, Dosa Racz does disclose

wherein the second perimeter firewall is between the endpoint device and the second access point server **(paragraph [0052] and Fig. 3, Dosa Racz teaches a firewall between a client device and a gateway.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Dosa Racz for having the second perimeter firewall be between the endpoint device and the second access point server because this would improve flexibility, offload processing burden, and allow for efficient replacement of malfunctioning firewall equipment.

As to **claim 28**, the combination of teachings between Uchida and Feghali disclose the multi-perimeter firewall system according to claim 14. While the combination of teachings between Uchida and Feghali does disclose two firewalls in between devices (see for example Figs. 1 and 3 of Uchida and Fig. 1 of Feghali), the combination of teachings between Uchida and Feghali is not explicitly clear on disclosing wherein the first perimeter firewall is between the first access point server and the second access point server as claimed. However, Dosa Racz does disclose

wherein the first perimeter firewall is between the first access point server and the second access point server **(paragraph [0052] and Fig. 3, Dosa Racz teaches a firewall between a gateway and a server.)**.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the modified invention of Uchida with the teachings of Dosa Racz for having the first perimeter firewall be between the first access point server and the second access point server because this would improve flexibility, offload processing burden, and allow for efficient replacement of malfunctioning firewall equipment.

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Walter et al. (U.S. Pub. No. 2010/0131616) – Fig. 1
- b. Cornelius et al. (U.S. Pub. No. 7,254,833) – Fig. 1
- c. Pietsch et al. ((U.S. Pub. No. 2007/0226043) – Fig. 1

27. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THADDEUS J PLECHA whose telephone number is (571)270-7506. The examiner can normally be reached on M-F 8-4:30.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THADDEUS J PLECHA/
Examiner, Art Unit 2438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Carlos Eduardo Oré et al. Confirmation No.: 8292
Application No.: 15/563,261 Art Unit: 2438
Filed: September 29, 2017 Examiner: T. J. Plecha
Title: MULTI-PERIMETER FIREWALL IN THE CLOUD

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AFTER FINAL ACTION UNDER 37 C.F.R. § 1.116

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Office Action dated March 22, 2019, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently amended) A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:

an egress ingress point device;

a first access point server in communication with the egress ingress point device;

a second access point server in communication with the first access point sever;

an endpoint device in communication with the second access point server;

a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent[[s]] at least some traffic from passing from the first access point server to the second access point server; and

a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent[[s]] at least some traffic from passing from the second access point server to the end point device,

wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware.

2. (Previously presented) The multi-perimeter firewall system according to claim 1, wherein at least one of the access point servers is configured to perform firewall services.

3. (Previously presented) The multi-perimeter firewall system according to claim 1, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path.

4. (Previously presented) The multi-perimeter firewall system according to claim 3, wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel.

5. (Previously presented) The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a global virtual network back channel.
6. (Previously presented) The multi-perimeter firewall system according to claim 3, wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.
7. (Previously presented) The multi-perimeter firewall system according to claim 6, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.
8. (Canceled)
9. (Currently amended) The multi-perimeter firewall system according to claim [[8]] 1, wherein the deep packet inspection is performed on flow through traffic.
10. (Currently amended) The multi-perimeter firewall system according to claim 8, wherein the deep packet inspection is performed on a cloned copy of traffic that flows through ~~the at least one of the first perimeter firewall and the second perimeter firewall.~~
- 11-12. (Canceled)
13. (Previously presented) The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.
14. (Currently amended) A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:
 - an egress ingress point device;

a first access point server in communication with the egress ingress point device;
a second access point server in communication with the first access point sever;
an endpoint device in communication with the second access point server;
a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent[[s]] at least some traffic from passing from the first access point server to the second access point server using a first firewall mechanism; and

a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent[[s]] at least some traffic from passing from the second access point server to the end point device using a second, different firewall mechanism,

wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware.

15. (Previously presented) The multi-perimeter firewall system according to claim 14, wherein at least one of the access point servers is configured to perform firewall services.

16. (Previously presented) The multi-perimeter firewall system according to claim 14, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path.

17. (Previously presented) The multi-perimeter firewall system according to claim 16, wherein the communication path between the first firewall and the second firewall is a global virtual network tunnel.

18. (Previously presented) The multi-perimeter firewall system according to claim 16, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a global virtual network back channel.

19. (Previously presented) The multi-perimeter firewall system according to claim 16, wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.
20. (Previously presented) The multi-perimeter firewall system according to claim 19, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.
21. (Canceled)
22. (Currently amended) The multi-perimeter firewall system according to claim ~~[[21]]~~ 14, wherein the deep packet inspection is performed on flow through traffic.
23. (Currently amended) The multi-perimeter firewall system according to claim 21, wherein the deep packet inspection is performed on a cloned copy of traffic that flows through ~~the at least one of the first perimeter firewall and the second perimeter firewall.~~
- 24-25. (Canceled)
26. (Previously presented) The multi-perimeter firewall system according to claim 14, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.
27. (Previously presented) The multi-perimeter firewall system according to claim 14, wherein the second perimeter firewall is between the endpoint device and the second access point server.
28. (Previously presented) The multi-perimeter firewall system according to claim 14, wherein the first perimeter firewall is between the first access point server and the second access point server.

29. (New) The multi-perimeter firewall system according to claim 1, wherein the egress ingress point device receives traffic directly from the Internet.
30. (New) The multi-perimeter firewall system according to claim 1, wherein the first perimeter firewall is coupled to a multi-honed backbone.
31. (New) The multi-perimeter firewall system according to claim 1, wherein the at least some traffic prevented from passing from the first access point server to the second access point server includes traffic with recognized malicious headers.
32. (New) The multi-perimeter firewall system according to claim 14, wherein the egress ingress point device receives traffic directly from the Internet.
33. (New) The multi-perimeter firewall system according to claim 14, wherein the first perimeter firewall is coupled to a multi-honed backbone.
34. (New) The multi-perimeter firewall system according to claim 14, wherein the at least some traffic prevented from passing from the first access point server to the second access point server includes traffic with recognized malicious headers.

REMARKS

I. Status of the Claims

Claims 1-28 were pending in the present application (the “Application”). In this response, Applicant has amended claims 1, 9, 10, 14, 22, and 23, canceled claims 8, 11, 12, 21, 24, and 25 without prejudice, and added new claims 29-34. Support for the claim amendments can be found throughout the as-filed specification including, for example, paragraphs [0129]-[0133] and [0169]. No new matter has been added. Upon entry of the amendments, claims 1-7, 9, 10, 13-20, 22, 23, and 26-34 will be pending. Applicant respectfully requests reconsideration and allowance of the Application in view of the claim amendments and the following comments.

II. Claim Objections

Claims 21-23 are objected to as being duplicate claims of claims 8-10. The Office Action suggests the dependency of claim 21 be changed from claim 1 to claim 14 so as to no longer be a duplicate claim. By this Amendment, Applicant cancels claim 21 without prejudice and amends claim 22 to depend from claim 14 as suggested, thereby addressing the grounds for the objections. Applicant respectfully requests that the objections be withdrawn.

III. Claim Rejections - 35 U.S.C. § 101

Claims 1-28 stand rejected under 35 U.S.C. § 101 as failing to fall within one of the four statutory categories of invention. Specifically, the Office Action states that “[n]one of the claimed devices, servers, or firewalls are specifically defined in the claims or in the instant specification as being hardware.” (Office Action, p. 8). The Office Action suggests that the rejection may be overcome by “specifically defining one or more of the devices, servers, and firewalls as hardware.” (*Id.*). By this Amendment, Applicant amends claims 1 and 14 to recite that “at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware.” These amendments are supported by at least paragraph [0169] and FIG. 22 of the specification. (*See, e.g.*, paragraph [0169] (“The lowest level of each device are the memory (RAM) S106, S206, S306, S406 and processors (CPU) S102, S202, S302, S402 and the network interfaces (NIC) S108, S208,

S308, S408. All of these are on the hardware level”)). Applicant respectfully submits that these amendments address the grounds for rejection.

Thus, amended claims 1 and 14 are statutory. Dependent claims 2-13 and 15-28 depend from claims 1 or 14 and are therefore statutory at least based on their dependency. Applicant respectfully requests that the Examiner reconsider and withdraw these rejections.

IV. Claim Rejections - 35 U.S.C. § 103

A. Claims 1-3, 8, 9, 14-16, 21, and 22

Claims 1-3, 8, 9, 14-16, 21 and 22 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over U.S. Publication No. 2002/0046253 to Uchida et al. (“Uchida”) in view of U.S. Publication No. 2015/0128246 to Feghali et al. (“Feghali”). Applicant respectfully traverses these rejections in view of the following comments.

Claim 1

Independent claim 1, as amended, recites “a first perimeter firewall in communication with the first access point server, wherein *the first perimeter firewall performs stateful packet inspection* to prevent at least some traffic from passing from the first access point server to the second access point server; and a second perimeter firewall in communication with the second access point server, wherein the *second perimeter firewall performs deep packet inspection* to prevent at least some traffic from passing from the second access point server to the end point device.” (Emphases added). This distributed arrangement of the first perimeter firewall and the second perimeter firewall “offers the opportunity to distribute both types of packet inspection [*e.g.*, stateful packet inspection and deep packet inspection] at various points in the cloud.” (Specification, [0132]). As one non-limiting example, the claimed first perimeter firewall that performs stateful packet inspection may be located at the closest edge to the Internet such that the “bulk amount of attack traffic from known source IP addresses or with recognized malicious headers can be thwarted.” (*Id.*, [0133]). “[A]t this first perimeter, attacks can be caught, protecting bandwidth within the GVN.” (*Id.*). The claimed second perimeter firewall that performs deep packet inspection “can be a trailing indicator allowing certain traffic through but analyzing and recording the results.” (*Id.*, [0134]).

Amended claim 1 incorporates at least some features of previously presented claims 11 and 12, which depended from claim 1. Claims 11 and 12 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2005/0235352 to Staats et al. (“Staats”). Accordingly, the comments below address the teachings of Uchida and Feghali, as applied to claim 1, and Staats, as applied to claims 11 and 12.

Uchida discloses “a highly secured electronic file management system under which a plurality of users can supply data to a database server of an enterprise.” (Uchida, [0001]). “[D]ata sent from users are received by the internal server 33 and protected from unauthorized access from the outside, by existence of the two-stage firewalls and private line.” (*Id.*, [0065]).

Feghali discloses “[a] network [that] is connected to an external network by a number of firewalls.” (Feghali, Abstract). Feghali further discloses that “[i]n some configurations, multiple firewalls 150 from different suppliers are placed in series in an attempt to overcome deficiencies in any one supplier's device, such as an inadequate rule set or programming errors that allow undesirable traffic to ‘leak’ through it.” (*Id.*, [0030]). In addition, Feghali teaches that a firewall may block traffic on a per-session basis “based on information gleaned during the session (e.g., from “deep packet inspection”).” (*Id.*, [0138]).

Staats discloses “[a] system 10 [that] may be utilized to provide a company with critical information technology (IT) services for installing, connecting, managing and securing their network environment without having to rely on several discrete systems.” (Staats, [0026]). “[S]ystem 10 includes a management center 12 and at least one device 14 in communication with the management center 12 via the Internet 16.” (*Id.*, [0027]). “[A] firewall module 54 of the device 14 is operable to provide the device 14 with firewall functionality.” (*Id.*, [0033]).

Referring to previously presented claims 11 and 12, the Office Action relies on Staats to allegedly teach limitations associated with “stateful packet inspection,” and separately, the Office Action relies on Feghali to allegedly teach limitations associated with “deep packet inspection.” (Office Action, p. 23). However, even assuming *arguendo* that Staats teaches “stateful packet inspection” and Feghali teaches “deep packet inspection,” which Applicant does not concede, the

cited references do not further teach or suggest the claimed arrangement of a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” where the first and second perimeter firewalls are distributed such that the “first perimeter firewall [is] in communication with the first access point server” and the “second perimeter firewall [is] in communication with the second access point server,” as recited by amended claim 1.

More specifically, to the extent that Feghali generally refers to the process of deep packet inspection, Feghali is silent regarding “stateful packet inspection.” Therefore, Feghali does not teach or suggest any arrangement of a first perimeter firewall that performs stateful packet inspection and a second perimeter firewall that performs deep packet inspection, much less the claimed arrangement of the first and second perimeter firewalls where the first and second perimeter firewalls are distributed such that the “first perimeter firewall [is] in communication with the first access point server” and the “second perimeter firewall [is] in communication with the second access point server,” as recited by amended claim 1.

Staats is unable to cure the above-identified deficiencies of Feghali. As discussed above, Staats teaches that “the firewall module 54 allows for the device 14 to perform deep packet inspection [and] stateful inspection.” (Staats, [0033]). Consequently, Staats teaches a single component (firewall module 54) that is capable of both stateful inspection and deep packet inspection rather than the claimed arrangement of a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” where the first and second perimeter firewalls are distributed such that the “first perimeter firewall [is] in communication with the first access point server” and the “second perimeter firewall [is] in communication with the second access point server,” as recited by amended claim 1. For example, the firewall module 54 of Staats, which performs both stateful packet inspection and deep packet inspection at a single location, does not allow a distributed arrangement that provides a first perimeter at which attacks can be caught using stateful packet inspection and a second perimeter at which a trailing indicator is provided using deep packet inspection. (*Cf.* Specification, [0133]-[0134]). Uchida is unable to cure the above-identified deficiencies of Feghali and Staats because

Uchida is silent regarding stateful packet inspection and deep packet inspection, and the Office Action does not cite Uchida for these claimed features.

Accordingly, Uchida, Feghali, and Staats, alone or in combination, do not teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

Thus, amended claim 1 is allowable over Uchida, Feghali, and Staats. Applicant respectfully requests that the Office reconsider and withdraw this rejection.

Claim 14

Independent claim 14, as amended, recites limitations that are substantially similar to those of claim 1 discussed above. Accordingly, claim 14 is patentable over Uchida, Feghali, and Staats for at least the same reasons as claim 1. Applicant respectfully requests that the Office reconsider and withdraw this rejection.

Claims 2, 3, 9, 15, 16, and 22

Each of dependent claims 2, 3, 9, 15, 16, and 22 depends, directly or indirectly, from claim 1 or claim 14. Accordingly, each of these dependent claims is also patentable over Uchida, Feghali, and Staats, at least based on their dependency. Applicant respectfully requests that the Office reconsider and withdraw these rejections.

Claims 8 and 22

Applicant cancels claims 8 and 21 without prejudice, thereby rendering these rejections moot.

B. Claims 4 and 17

Claims 4 and 17 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2010/0325309 to Cicic et al. (“Cicic”). Applicant respectfully traverses these rejections in view of the following comments.

Each of claims 4 and 17 depends, directly or indirectly, from claim 1 or claim 14. Accordingly, each of these dependent claims is also patentable over Uchida and Feghali, at least based on their dependency.

Cicic fails to cure the above-identified deficiencies of Uchida and Feghali discussed in connection with claims 1 and 14. Cicic generally discloses “[a] global virtual network with guaranteed capacity [that] is used to transport... IP packets.” (Cicic, Abstract). “Firewalls are used to enforce security in the local network.” (*Id.*, [0031]).

The Office Action relies on Cicic to teach limitations related to a “global virtual network tunnel.” (Office Action, p. 15). Applicant disagrees that Cicic teaches these limitations. However, even assuming *arguendo* that Cicic teaches a “global virtual network tunnel,” Cicic does not further teach or suggest a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” as recited by amended claim 1. In fact, Cicic is silent regarding both stateful packet inspection and deep packet inspection, and the Office Action does not cite Cicic for these claimed features. Accordingly, Cicic fails to teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

Thus, claims 4 and 17 are allowable over Uchida, Feghali, and Cicic. Applicant respectfully requests that the Office reconsider and withdraw the rejections

C. Claims 5 and 18

Claims 5 and 18 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2014/0210693 Bhamidipati et al. (“Bhamidipati”). Applicant respectfully traverses these rejections in view of the following comments.

Each of claims 5 and 18 depends, directly or indirectly, from claim 1 or claim 14. Accordingly, each of these dependent claims is also patentable over Uchida and Feghali, at least based on their dependency.

Bhamidipati fails to cure the above-identified deficiencies of Uchida and Feghali. Bhamidipati generally discloses “a reverse channel architecture referred to as the Wi-Fi User Input Back Channel (UIBC) that has been modified to transport one or more additional input types over UDP.” (Bhamidipati, Abstract). Bhamidipati further teaches that “UIBC may be extended to transport voice input and VNC input types.” (*Id.*).

The Office Action relies on Bhamidipati to teach limitations related to a “global virtual network back channel.” (Office Action, p. 17). Applicant disagrees that Bhamidipati teaches these limitations. However, even assuming *arguendo* that Bhamidipati teaches a “global virtual network back channel,” Bhamidipati does not further teach or suggest a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” as recited by amended claim 1. In fact, Bhamidipati is silent regarding both stateful packet inspection and deep packet inspection, and the Office Action does not cite Bhamidipati for these claimed features. Accordingly, Bhamidipati fails to teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

Thus, claims 5 and 18 are allowable over Uchida, Feghali, and Bhamidipati. Applicant respectfully requests that the Office reconsider and withdraw the rejections

D. Claims 6 and 19

Claims 6 and 19 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2015/0326588 to Vissamsetty et al. (“Vissamsetty”). Applicant respectfully traverses these rejections in view of the following comments.

Each of claims 6 and 19 depends, directly or indirectly, from claim 1 or claim 14. Accordingly, each of these dependent claims is also patentable over Uchida and Feghali, at least based on their dependency.

Vissamsetty fails to cure the above-identified deficiencies of Uchida and Feghali. Vissamsetty generally discloses “systems and method for detecting and protecting malicious and unauthorized access of a computer system.” (Vissamsetty, [0003]). More specifically, Vissamsetty discloses “[a] system of client devices and a server system implementing services makes use of credentials to facilitate authentication of the client devices with the server and generates log entries for different accesses to the server system.” (*Id.*, Abstract).

The Office Action relies on Vissamsetty to teach limitations related to “shar[ing] threat information.” (Office Action, p. 18). Applicant disagrees that Vissamsetty teaches these limitations. However, even assuming *arguendo* that Vissamsetty teaches the sharing of threat information, Vissamsetty does not further teach or suggest a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” as recited by amended claim 1. In fact, Vissamsetty is silent regarding both stateful packet inspection and deep packet inspection, and the Office Action does not cite Vissamsetty for these claimed features. Accordingly, Vissamsetty fails to teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

Thus, claims 6 and 19 are allowable over Uchida, Feghali, and Vissamsetty. Applicant respectfully requests that the Office reconsider and withdraw the rejections.

E. Claims 7 and 20

Claims 7 and 20 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of (U.S. Publication No. 2015/0281176 to Banfield et al. (“Banfield”). Applicant respectfully traverses these rejections in view of the following comments.

Each of claims 7 and 20 depends, directly or indirectly, from claim 1 or claim 14. Accordingly, each of these dependent claims is also patentable over Uchida and Feghali, at least based on their dependency.

Banfield fails to cure the above-identified deficiencies of Uchida and Feghali. Banfield generally discloses “[a] network of firewall devices [that] collects analysis data from all firewall devices in the network, and transmits it to a central server system.” (Banfield, Abstract). Banfield further discloses that “[t]he central server system will continually distribute new threat and update information to the networked firewall devices.” (*Id.*).

The Office Action relies on Banfield to teach limitations related to “shar[ing] threat information with a central control server.” (Office Action, p. 20). Applicant disagrees that Banfield teaches these limitations. However, even assuming *arguendo* that Banfield teaches the sharing of threat information with a central control server, Banfield does not further teach or suggest a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” as recited by amended claim 1. In fact, Banfield is silent regarding both stateful packet inspection and deep packet inspection, and the Office Action does not cite Banfield for these claimed features. Accordingly, Banfield fails to teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

Thus, claims 7 and 20 are allowable over Uchida, Feghali, and Banfield. Applicant respectfully requests that the Office reconsider and withdraw the rejections.

F. Claims 10 and 23

Claims 10 and 23 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2016/0337484 to Tola (“Tola”). Applicant respectfully traverses these rejections in view of the following comments.

Each of claims 10 and 23 depends, directly or indirectly, from claim 1 or claim 14. Accordingly, each of these dependent claims is also patentable over Uchida and Feghali, at least based on their dependency.

Tola fails to cure the above-identified deficiencies of Uchida and Feghali. Tola generally discloses “an adaptable framework that removes operating system restrictions from network

communications.” (Tola, [0033]). The system of Tola is designed to “provide encryption options, isolate the network from the operating system, and yet simultaneously be transparent to the operating system in order to avoid any interaction issues, for example with applications executing in the operating system environment.” (*Id.*). Tola further discloses “[d]ynamic firewall features [that are] similar to deep packet inspection firewalls, although with numerous differentiating features.” (*Id.*, [0084]).

The Office Action relies on Tola to teach limitations related to a “deep packet inspection... performed on a cloned copy of traffic.” (Office Action, p. 21). Applicant disagrees that Tola teaches these limitations. However, even assuming *arguendo* that Tola teaches deep packet inspection performed on a cloned copy of traffic, Tola does not further teach or suggest a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” as recited by amended claim 1. To the extent that Tola may generally refer to the process of deep packet inspection, Tola is silent regarding stateful packet inspection, and the Office Action does not cite Tola for this claimed feature. Therefore, Tola does not teach or suggest arrangements of firewalls that perform both stateful packet inspection and deep packet inspection, much less the claimed arrangement recited by amended claim 1. Accordingly, Tola fails to teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

Thus, claims 7 and 20 are allowable over Uchida, Feghali, and Banfield. Applicant respectfully requests that the Office reconsider and withdraw the rejections.

G. Claims 11, 12, 24, and 25

Claims 11, 12, 24, and 25 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2005/0235352 to Staats et al. (“Staats”). Applicant cancels claims 11, 12, 24, and 25, rendering these rejections moot.

H. Claims 13 and 26

Claims 13 and 26 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Uchida in view of Feghali, and further in view of U.S. Publication No. 2012/0210417 to Shieh (“Shieh”). Applicant respectfully traverses these rejections in view of the following comments.

Each of claims 13 and 26 depends, directly or indirectly, from claim 1 or claim 14. Accordingly, each of these dependent claims is also patentable over Uchida and Feghali, at least based on their dependency.

Shieh fails to cure the above-identified deficiencies of Uchida and Feghali. Shieh generally discloses “a distributed firewall using virtual machines..” (Shieh, [0002]). Shieh’s distributed firewall “includes at least one IO module for performing IO functionality of the distributed firewall, at least one security processing module for performing security functionality of the distributed firewall and a firewall controller for managing the IO module and the security processing module.” (*Id.*, Abstract). “Examples of the firewall functions include, but are not limited to, network address translation (NAT), virtual private network (VPN), deep packet inspection (DPI), and/or anti-virus, etc.” (*Id.*, [0022]).

The Office Action relies on Shieh to teach limitations related to a “cloud firewall load balancer.” (Office Action, p. 25). Applicant disagrees that Shieh teaches these limitations. However, even assuming *arguendo* that Shieh teaches a “cloud firewall load balancer,” Shieh does not further teach or suggest a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” as recited by amended claim 1. To the extent that Shieh may generally refer to the process of deep packet inspection, Shieh is silent regarding stateful packet inspection, and the Office Action does not cite Shieh for this claimed feature. Therefore, Shieh does not teach or suggest arrangements of firewalls that perform both stateful packet inspection and deep packet inspection, much less the claimed arrangement recited by amended claim 1. Accordingly, Shieh fails to teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

Thus, claims 13 and 26 are allowable over Uchida, Feghali, and Shieh. Applicant respectfully requests that the Office reconsider and withdraw the rejections.

V. New Claims

Each of new dependent claims 29-34 depends, directly or indirectly, from claims 1 or 14. Accordingly, each of these dependent claims is also allowable, at least based on their dependency. Applicant respectfully requests allowance of the new claims.

CONCLUSION

In view of the above amendment, applicant believes the pending application is in condition for allowance.

The fee for a two-month extension of time is submitted herewith. Applicant believes no additional fee is due with this response. However, in the event the U.S. Patent and Trademark Office determines that an additional fee is required, Applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 08-0219 under Order No. 2210592.02089US5.

Respectfully submitted,

Dated: August 21, 2019

/Yu Yang/
Yu Yang
Registration No.: 68,839
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23483 7590 10/17/2019
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

EXAMINER	
PLECHA, THADDEUS J	
ART UNIT	PAPER NUMBER

2438

DATE MAILED: 10/17/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/563,261	09/29/2017	Carlos Eduardo ORÉ	2210592.02089US5	8292

TITLE OF INVENTION: MULTI-PERIMETER FIREWALL IN THE CLOUD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	01/17/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

23483 7590 10/17/2019
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/563,261	09/29/2017	Carlos Eduardo ORÉ	2210592.02089US5	8292

TITLE OF INVENTION: MULTI-PERIMETER FIREWALL IN THE CLOUD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	01/17/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
PLECHA, THADDEUS J	2438	726-011000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

1 _____

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/563,261	09/29/2017	Carlos Eduardo ORÉ	2210592.02089US5	8292
23483	7590	10/17/2019	EXAMINER	
WILMERHALE/BOSTON			PLECHA, THADDEUS J	
60 STATE STREET			ART UNIT	
BOSTON, MA 02109			PAPER NUMBER	
			2438	
DATE MAILED: 10/17/2019				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, ^{Cisco v. Umbra} ~~or local~~ ^{EX-1002-0003} enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/563,261	Applicant(s) ORÉ et al.	
	Examiner THADDEUS J PLECHA	Art Unit 2438	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to communications received 21 August 2019 and 18 September 2019.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are See Continuation Sheet. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov**.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. ____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892) 2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>9/18/2019</u> . 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____. 4. ☒ Interview Summary (PTO-413), Paper No./Mail Date <u>10/11/2019</u> .	5. ☒ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
---	---

/THADDEUS J PLECHA/
Examiner, Art Unit 2438

Continuation of 3. The allowed claim(s) is/are: 1-7,9,13-20,22 and 26-34

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.
2. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.
3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
4. This Office Action is in response to amendments filed on August 21, 2019. Claims 1, 9, 10, 14, 22 and 23 have been amended. Claims 8, 11, 12, 21, 24 and 25 have been newly cancelled. Claims 29-34 have been newly added. Therefore, claims 1-7, 9, 10, 13-20, 22, 23 and 26-34 are pending and addressed below.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/18/2019 has been entered.

Response to Arguments

6. Applicant's amendments are sufficient to overcome the claim objections for claims 21-23 set forth in the previous Office Action but not all the objections.
7. Applicant's amendments are sufficient to overcome the claim rejections under 35 U.S.C. 101 for claims 1-28 set forth in the previous Office Action.
8. Applicant's amendments (and Examiner's amendments herein below) are sufficient to overcome the claim rejections under 35 U.S.C.103 set forth in the previous Office Action.

EXAMINER'S AMENDMENT

9. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in an interview with Yu Yang (Reg. No. 68,839) on 11 October 2019.

The application has been amended as follows:

Listing of Claims:

Claim 1 (Currently Amended) A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:
an egress ingress point device;

a first access point server in communication with the egress ingress point device;

a second access point server in communication with the first access point sever;

an endpoint device in communication with the second access point server;

a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and

a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,

wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware,

wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.

Claim 4 (Currently Amended) The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a ~~global-virtual~~ network path tunnel.

Claim 5 (Currently Amended) The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a ~~global virtual~~ network back channel.

Claim 10 (Cancelled)

Claim 14 (Currently Amended) A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:

an egress ingress point device;

a first access point server in communication with the egress ingress point device;

a second access point server in communication with the first access point sever;

an endpoint device in communication with the second access point server;

a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server using a first firewall mechanism; and

a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device using a second, different firewall mechanism,

wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware,

wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.

Claim 17 (Currently Amended) The multi-perimeter firewall system according to claim 16, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a ~~global-virtual~~ network path tunnel.

Claim 18 (Currently Amended) The multi-perimeter firewall system according to claim 16, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a ~~global-virtual~~ network back channel.

Claim 23 (Cancelled)

Allowable Subject Matter

10. Independent claims 1 and 14 are allowed. Dependent claims 2-7, 9, 13, 15-20, 22 and 26-34 are allowed based on their dependency.

11. The following is an examiner's statement of reasons for allowance:

12. Claim 1 recites, *inter alia*, “a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device... wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.”

13. The closest prior arts made of record are:

- i) Uchida et al. (U.S. Pub. No. 2002/0046253 and hereinafter referred to as Uchida) which discloses two firewalls (paragraphs [0005], [0006], [0048] and [0065] and Figs. 1 and 3 of Uchida).
- ii) Feghali et al. (U.S. Pub. No. 2015/0128246 and hereinafter referred to as Feghali) which discloses multiple firewalls connected in series where each firewall controls data coming into and going out of a network (paragraphs [0029]-[0030] and Fig. 1 of Feghali).
- iii) Staats et al. (U.S. Pub. No. 2005/0235352 and hereinafter referred to as Staats) which discloses a firewall performing deep and stateful inspection (paragraph [0033] of Staats).

14. None of the prior art anticipates or makes obvious the invention of the present application before the effective filing date of the claimed invention, the invention including: “a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device... wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall” (as recited in claim 1). Therefore, claim 1 is considered to be allowable.

15. Claim 14, although different, recites substantially similar subject matter to claim 1 and is therefore allowable for the same reasons as discussed with claim 1 above.

16. None 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 before the effective filing date of the claimed invention.

17. Any comments considered necessary by applicant must be submitted no later than payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Kasdon (U.S. Pub. No. 2014/0278543) – Fig. 2
- b. McDonald et al. (U.S. Pub. No. 2002/0087447) – Fig. 1
- c. Lee (U.S. Pub. No. 2008/0301794) – Fig. 2

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THADDEUS J PLECHA whose telephone number is (571)270-7506. The examiner can normally be reached on M-F 8-4:30.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THADDEUS J PLECHA/
Examiner, Art Unit 2438