UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

Case IPR2019-00820
Patent 7,937,581

PATENT OWNER'S SUR-REPLY TO PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. THE SECURITY FLAW IN ISHIYAMA'S REQUEST MESSAGE WOULD PREVENT IT FROM EVER BEING USED TO CONSTRUCT A SYSTEM FOR SECURE COMMUNICATION 2

A. The Request Message Of Ishiyama Identified By Petitioner As The Claimed Request Message Has A Fatal Security Defect 2

B. The Deposition Testimony Of Dr. Rouskas Confirms The Security Flaw In Ishiyama..6

C. The Security Defect Prevents Ishiyama From Meeting The Core Requirements Of An Obviousness Case 9

III. CONSTRUCTION OF THE TERM "SECURITY GATEWAY" 11

IV. PETITIONER FAILS TO DEMONSTRATE THAT ISHIYAMA AND MURAKAWA DISCLOSE THE CLAIMED "SECURITY GATEWAY" 13

A. Petitioner's New Theory, That Ishiyama's Correspondent Host Could Be Modified To Be A Security Gateway Because It Was The Only Other Option, Should be Rejected....................14

B. Petitioner's Misleading Argument That The Care-Of Address Referred To As The "Gateway Address" Of The Mobile Terminal In Ishiyama Is Actually A Security Gateway Should Be Rejected 16

C. None Of Petitioner's Other Miscellaneous Arguments Is Persuasive..17

V. PETITIONER FAILS TO DEMONSTRATE HOW ISHIYAMA AND MURAKAWA COULD BE COMBINED 19

VI. CLAIMS 3 AND 5 HAVE NOT BEEN SHOWN TO BE UNPATENTABLE 21

A. Claims 3 And 5 Were Challenged Under Ground 2 And Petitioner Cannot Amend Its Petition To Challenge Them Under Ground 1 21

B. Claims 3 And 5 Are Not Unpatentable Under Ground 2 Because Ahonen Fails To Teach Or Suggest The Recited "Reply Message" 22

VII. CLAIMS 6-8 ARE PATENTABLE OVER THE APPLIED REFERENCES 25

VIII. CONCLUSION 26

TABLE OF AUTHORITIES

Page(s)

CASES

Henny Penny Corporation v. Frymaster LLC,
938 F.3d 1324 (Fed. Cir. 2019) 14

In re Smith International, Inc.,
871 F.3d 1375 (Fed. Cir. 2017) 18

Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.,
821 F.3d 1359 (Fed. Cir. 2016) 14

KSR Int'l Co. v. Teleflex Inc.,
127 S.Ct. 1727 (2007)..9

Personal Webs. Techs., LLC v Apple, Inc.,
848 F.3d 987 (Fed. Cir. 2017) 20

Personalized Media Communications, LLC v. Apple Inc.,
952 F.3d 1336 (Fed. Cir. 2020) 12

Pfizer, Inc. v. Apotex, Inc.,
480 F.3d 1348 (Fed. Cir. 2007) 9

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) 12

Regents of Univ. of California v. Broad Institute, Inc.,
903 F.3d 1286 (Fed. Cir. 2018) 9

Wi-LAN USA, Inc. v. Apple Inc.,
830 F.3d 1374 (Fed. Cir. 2016) 12

REGULATIONS

37 C.F.R. § 42.23(b) 1, 14

EXHIBIT LIST	
2001	Network Working Group Request for Comments: 2002 (C. Perkins, ed.) (Oct. 1996) (“RFC 2002”).
2002	Declaration of Richard B. Megley, Jr. (“Megley Decl.”).
2009	Petition in IPR2019-00819
2004	CV of George N. Rouskas
2005	Network Working Group Request for Comments: 1122 (R. Braden, ed.) (Oct. 1989), “Requirements for Internet Hosts -- Communication Layers” (RFC 1122)
2006	Declaration of Stephen T. Schreiner (“Schreiner dec.”)
2007	Ex. 1003 (Declaration of Dr. Goldschlag) from Apple v. MPH Techs. Oy IPR2019-00821
2008	Deposition Transcript of Dr. Goldschlag (12-17-2019)
2009	Declaration of George N. Rouskas

I. INTRODUCTION

The Petition should be denied for all the reasons stated in Patent Owner's Response (POR), and also because Petitioner's Reply reveals a major security flaw in Ishiyama that would prevent it from ever being used by a POSITA as a reference to construct a secure communication system. Specifically, the new source address in the outer packet of Ishiyama's message alleged to be the request message of the claim is unencrypted and sent in the clear. Accordingly, a POSITA would never use Ishiyama's outer packet to change the address definition for the mobile device in a secure connection because it could easily be intercepted by a malicious intermediary and manipulated to cause message traffic to be misdirected to an imposter device.

In its Reply Petitioner still completely fails to explain exactly how Ishiyama and Murakawa are combined, what modifications are required and how the resulting combination would operate. Petitioner simply asserts that the references **could** be combined in some unspecified fashion without explaining **how** they are combined. That is not good enough.

Petitioner floats several new theories and even new grounds that should be rejected by the Board as untimely. Under 37 C.F.R. § 42.23(b), a reply cannot be used to belatedly submit new arguments, contentions or evidence to make out a *prima facie* case of unpatentability. A reply may only respond to arguments raised in the corresponding patent owner response. *Id.*

The Board should decline to consider Petitioner's new theories, new evidence, and new grounds.

II. THE SECURITY FLAW IN ISHIYAMA'S REQUEST MESSAGE WOULD PREVENT IT FROM EVER BEING USED TO CONSTRUCT A SYSTEM FOR SECURE COMMUNICATION

A. The Request Message Of Ishiyama Identified By Petitioner As The Claimed Request Message Has A Fatal Security Defect

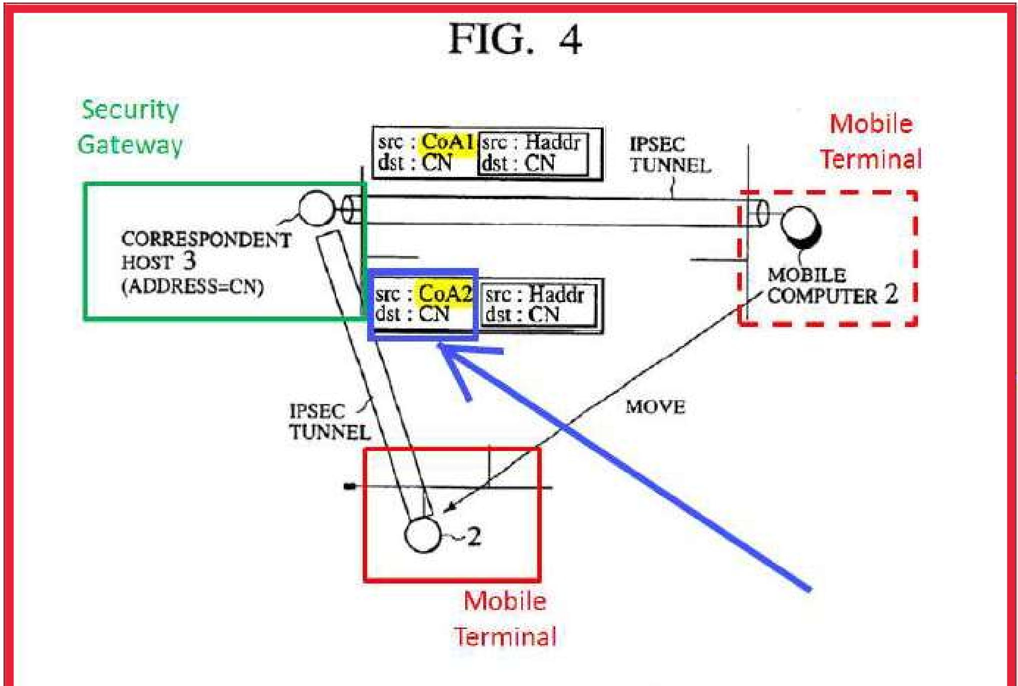
The Petitioner asserts in the Reply that the request message of claims 1 and 9 of the '581 Patent is Ishiyama's outer header containing the new source address CoA2 in the encapsulated packet sent from the mobile host (MH) to the correspondent host (CH). See Reply 14-15, 18-19 (citing Ishiyama's outer packet with updated source address CoA2 as being the request message that is appended to the encrypted inner packet) (citing to Pet., 31-33); Pet. 31 ("the request message . . . to change the security association definition from CoA1 to CoA2" is "the mobile computer 2 chang[ing] the source address of the outer packet of the encapsulated packet . . . into 'CoA2'")).

The supplemental declaration of Petitioner's expert (see Ex. 1022 [Goldschlag Reply Decl.] ¶ 61) cites Ishiyama 8:55-9:4, as describing the alleged request in Figure 4 as being the outer packet (outer header) with the source address changed from source address CoA1 to CoA2:

> Next, when the mobile computer 2 moves further and the Care-of address is changed from 'CoA1' to 'CoA2' as shown in FIG. 4, the **address changing is carried out as follows**. In this case, the mobile computer 2 **changes the source address of the outer packet of the encapsulated packet to be transmitted . . . by the mobile computer 2 into 'CoA2'** . . . As a result, as shown in FIG. 4, the encapsulated packet in which the outer packet has the source address ='CoA2' will be transferred. The correspondent host 3 that detected this change of the Care-of address of the mobile computer then replace[s] the destination gateway address 'CoA1' used so far in this session by a new one 'CoA2' by referring to the IPSEC security association (security related information) database (see FIG. 9B and FIG. 9D).

Ex. 1004, 0014 (8:55-9:10) (emph. added). Likewise, the Board referenced the requested address change in "setting a new current location address as the source address of the outer packet . . . to update the current location address." Paper 10 [Institution] 21 (citing to claim 1 of Ishiyama).

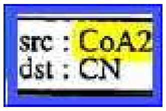
The outer header containing the source address that has been updated to CoA2 from CoA1 is shown in Figure 4 from Petitioner's expert declaration:



EX1004. FIG. 4 (annotated).

Ex. 1022 [Goldschlag Reply Decl.] ¶ 49 (Ishiyama Fig. 4 annotated in green/red by Petitioner; blue added by Patent Owner).

The alleged request message in Ishiyama, excerpted below, is the outer header containing the new source address information:



src : CoA2
dst : CN

Hereinafter, this message shall be referred to as the "New Source Address Outer Header."

A POSITA would never use the New Source Address Outer Header sent from MH 2 to CH 3 in Ishiyama to change the secure connection definition because it would create a major security flaw.[1] The New Source Address Outer Header containing CoA2—is **unencrypted and sent in the clear**.[2] Consequently, a malicious party could easily intercept the message, change the source information from CoA2 to a different address (e.g., HackerX) and then forward the message to CH 3. CH 3 would then respond by reconfiguring the security parameters in its Security Association Database (SADB) so that all subsequent messages from CH 3 would be sent to the HackerX address instead of MH 2 at

[1] The Petitioner was aware of the security flaw (see March 20, 2020, deposition of Dr. Rouskas) well in advance of the Reply (filed April 1, 2020). Neither the Reply nor its expert's supplemental declaration address the security flaw. See Ex. 1022 [Goldschlag Reply Decl.].

[2] There is no dispute that the outer header is unencrypted. Petitioner's counsel confirmed the point in deposition. Ex. 1021 [Dep. Tr. Rouskas] 97:8-11 (Q: "And in IPSec tunnel mode, the outer IP packet is transmitted in the clear, but the inner IP packet is encrypted. Is that right?" A: "That is correct."). See also Ex. 1002 [Goldschlag Decl.] ¶¶ 74-81; Ex. 1004, 0010 (Fig. 13), 0017 (13:59-14:10) (CH 3's mobile computer address management unit 136 for processing current address data from MH 2 is not connected to decryption unit 132).

CoA2. This would be a major security breach and completely undermines the goal of Ishiyama of providing secure communications between MH 2 and CH 3.

Furthermore, Ishiyama's failure to encrypt the New Source Address Outer Header means that Petitioner has not demonstrated that the alleged request message is encrypted, as set forth in dependent claim 4.

B. The Deposition Testimony Of Dr. Rouskas Confirms The Security Flaw In Ishiyama

Petitioner's counsel asked Dr. Rouskas in deposition how the message in Ishiyama functioned to change the definition of the secure connection as required by the claims. Dr. Rouskas responded that the message had a security flaw (objections omitted):

> Q: "And it [Ishiyama] explains that when the mobile hosts move between networks, the outer care-of address is changed from the old care-of address to the new care-of address. Right?"
> A: "That is correct. And it shows that the outer source address is changed from Care-of Address 1 to Care-of Address 2, and that it presents a major security flaw."

Ex. 1021 [Dep. Tr. Rouskas] 172:21-173:6, 174:5-11 (Q: "And specifically, right, at Line 66, Ishiyama explains how the correspondent host knows that the care-of address changes and how it performs an update to its security associations. Right? A: "Yes, I can see that. As I said, that's the major security flaw.")

During redirect Dr. Rouskas explained the security flaw in the New Source Address Outer Header (all emph. added, objections omitted):

> Q: "Can you describe for me the security flaw in Ishiyama that you were referencing?"
>
> A: ". . . Now, according to the method described in Ishiyama, the mobile hosts may simply change the address of the -- the source address of the outer packets from CoA1 to CoA2 to notify the correspondent host of its new care-of address. The problem with that is that . . . even if the mobile host does not move, and remains at Care-of Address 1, any of the routers in the path between the mobile host and the correspondent host who may have been compromised by a malicious user, may inspect of the contents of the header of the outer packet **which is sent in the clear**. And if they are programmed by this malicious user, they could replace the source address CoA1 with some address X of -- that may belong to the domain of -- of this malicious user, let's say imposter address. And when the correspondent nodes receives that packets, it will think that the mobile host was moved, where that is not the case. It will modify security association. And from that point on it will be sending packets rather -- instead of sending the packets to the real address of the mobile host, which is Care-of Address 1, to the new address that was put into the header by the malicious user.".

Ex. 1021 [Dep. Tr. Rouskas] 185:7-187:3.

> Q: "And what is it about using the source address information in the header of the outer packet that is problematic for purposes of redefining the secure connection?"
>
> A: "The essence of the problem is that the source address of the outer packet is sent in the clear, and therefore any malicious router in the path between the two nodes may modify that – that header.
>
> Q: "So when you say it's sent in the clear, is it encrypted?"
>
> A: "It is not encrypted, no."

Ex. 1021 [Dep. Tr. Rouskas] 190:22-191:12.

> Q: "If . . . a malicious user changed the source address in the outer header of this packet to address X, what would be the effect at the correspondent host in Ishiyama?"
>
> A: "The correspondent host would update its secure -- its SA definition to the new address X; and, therefore, all the packets that the correspondent host would generate towards the mobile host will end up to address X instead of the mobile host. So it will basically completely destroy the secure communication between the mobile host and the correspondent host."

Ex. 1021 [Dep. Tr. Rouskas] 192:4-18.

> Q: "Do you consider this flaw to be a fatal security flaw, in terms of Ishiyama providing a system for secure communications?"
>
> A: "As I mentioned in my earlier testimony, this is -- this is a crucial and a major security flaw, in the sense that it completely destroys the secure communication between the two hosts."

Ex. 1021 [Dep. Tr. Rouskas] 193:4-11.

C. The Security Defect Prevents Ishiyama From Meeting The Core Requirements Of An Obviousness Case

A finding of obviousness requires a showing that (a) the prior art teaches or suggests each claim limitation; (b) there exists an apparent reason to combine the prior art as proposed; and (c) a person of ordinary skill would have a reasonable expectation of success that the proposed combination would operate for its intended purpose. *See KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007); *Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1361 (Fed. Cir. 2007); *Regents of Univ. of California v. Broad Institute, Inc*., 903 F.3d 1286, 1291 (Fed. Cir. 2018).

Ishiyama, considered alone or with a secondary reference, fails to meet any of the three requirements. Petitioner relies on the New Source Outer Header from Ishiyama as being the claimed request message that redefines a secure connection. But this message with its unsecured CoA2 address value fails to meet the claim limitation for maintaining a "secure connection" for sending a "secure message." Ex. 1001 ['581 Patent] 0011-0012 (10:50-11:3) (claim 1), 0012 (12:1-22) (claim 9). Second, a POSITA would not have an apparent reason to use Ishiyama because the security flaw would produce an inherently unsecure communication system. Third, a POSITA would have no reasonable expectation of success because Ishiyama would produce the opposite of the intended goal of designing a secure communication system.

Dr. Rouskas confirmed each of these points in deposition (objections omitted):

> Q: "Given the testimony you just gave regarding the security flaw, can Ishiyama be used to provide a secure connection in a system that is directed to secure communications? . . ."
>
> A: "It is my opinion that Ishiyama cannot be used to build a system that would provide secure connection between two hosts or between any devices."

Ex. 1021 [Dep. Tr. Rouskas] 195:16-196:6.

> Q: "Would a person of ordinary skill in the art be motivated or inclined to use Ishiyama, alone or in combination with another system or reference, to build a secure communication system?"
>
> A: "No."
>
> Q: "And why is that?"
>
> A: "Because of this particular security flaw. A system that is built with this mechanism that we described, where you change the source address that is sent in the clear to modify the security association, would not be secure."

Ex. 1021 [Dep. Tr. Rouskas] 196:15-197:6.

> Q: "And would a person of ordinary skill in the art have reasonable expectation of success if he or she was to attempt to use Ishiyama alone or in combination with another system to create a system for secure communication?"
>
> A: "No."
>
> Q: "And why is that the case?"

> A: "Because the end result would not be a secure connection. This flaw would – this particular security flaw would prevent the connection to operating a secure manner."

Ex. 1021 [Dep. Tr. Rouskas] 197:7-197:22.

III. CONSTRUCTION OF THE TERM "SECURITY GATEWAY"

The POR proposes a construction for the claim term "security gateway" POR, 11. Petitioner admits that the term has a well-understood meaning but refuses to state it in plain English or offer an alternative construction. Reply, 2-3 ("the '581 Patent uses the term . . . in its common form as well understood in the art . . .").

The Reply does not challenge the support for Patent Owner's construction found in the claim language itself. POR, 11. As for the specification, one quote passage describes how a security gateway receives packets from a host on a first network and forwards them on to a security gateway at another network which delivers the packets to another host. POR, 12-13 (citing Ex. 1001 ['581 Patent] 0008 (3:14-62)). Petitioner does not dispute that the passage clearly distinguishes "hosts" from a "security gateway."

The Reply attempts to dismiss the citation to the '581 Patent in Figures 1-2 and Col. 8:55-63. Reply, 4. But Petitioner does not dispute that the security gateway implemented in Figure 1 by computer 2 has two communication interfaces, one interface to computer 1 and another interface to computer 3.

Petitioner also does not dispute that security gateway computer 2 is an intermediary between computer 1 and computer 3. Finally, Petitioner does not dispute that the security gateway forwards packets from one network on to another. See Reply, 4.

Petitioner complains that "[t]he '581 patent does not present any special definition for 'security gateway' . . ." Reply, 4. However, it is well-established that a patent does not have to provide a "special definition" of a claim term. Indeed, the consistent use of a claim term in the specification can "define claim terms by implication." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005) (*en banc*); *Wi-LAN USA, Inc. v. Apple Inc.*, 830 F.3d 1374, 1382 (Fed. Cir. 2016) ("Consistent use of a term in a particular way in the specification can inform the proper construction of that term."), *cert denied*, 137 S.Ct. 1213 (2017). That is the case here. The '581 Patent uses the term "security gateway" twenty-eight times and Petitioner fails to identify even one instance where the term is used inconsistently with Patent Owner's construction.

The Reply similarly quibbles that the prosecution history does not "provide a definition" of a security gateway. Reply, 4-5. Like the specification, the prosecution history is not required to expressly define a term to be relevant. *Personalized Media Communications, LLC v. Apple Inc.*, 952 F.3d 1336, 1340 (Fed. Cir. 2020) (prosecution history such as amendment or explanation informed the meaning of a term without an express definition). The POR cited a claim amendment in the parent application reciting "the mobile terminal sending a secure message . . . to the other terminal via the security gateway." POR, 14-15. The amendment describes a security gateway that has two interfaces—one to the "mobile terminal" and another to the "other terminal." Petitioner's assertion that this amendment does not recite a security gateway with multiple interfaces, see Reply, 4 (asserting that amendment does not require "numerous interfaces"), is just not true.

Patent Owner also cited to multiple prior art references—all but one of which were cited by the Petition--supporting Patent Owner's construction of "security gateway." These references include Murakawa (Ex. 1005), Ahonen (Ex. 1006), Frankel (Ex. 1008), RFC 1122 (Ex. 2005) and RFC 2401 (Ex. 1011). See POR, 17-24. Tellingly, Petitioner does not dispute—for even a single reference—the merits of Patent Owner's explanation of how each of these references describe and define "security gateway." Reply, 4-5.

IV. PETITIONER FAILS TO DEMONSTRATE THAT ISHIYAMA AND MURAKAWA DISCLOSE THE CLAIMED "SECURITY GATEWAY"

The Reply offers various theories—some found in its Petition, others newly concocted, as to why the unexplained Ishiyama/Murakawa combination discloses the claimed "security gateway." None closes the gaps in Petitioner's case.

A. Petitioner's New Theory, That Ishiyama's Correspondent Host Could Be Modified To Be A Security Gateway Because It Was The Only Other Option, Should be Rejected

The primary argument in the Petition was that Ishiyama's correspondent host 3 **is** a security gateway. Pet., 22. But Patent Owner explained that multiple references--including RFC 2401, Ahonen, and Frankel--describe correspondent hosts as being distinct from a security gateway in the field of network security. See POR, 33-34. Now Petitioner's Reply seems to advance a new theory, namely, that the correspondent host could be replaced by or modified to be a security gateway.

Petitioner argues for the first time that it would have been obvious "to modify Ishiyama's 'correspondent host' to be a 'security gateway.'" because IPsec endpoints have only two possible options: (1) a correspondent host or (2) a security gateway. Reply, 5. Nowhere does the Petition argue or submit evidence that Ishiyama's correspondent host should be modified to be a security gateway based on a limited number of endpoints. This new theory and the evidence in support of it (see Ex. 1022 [Goldschlag Reply Decl.] (¶ 15-25)) should not be considered by the Board. 37 C.F.R. § 42.23(b); November 2019 Consolidated Trial Practice Guide ("Trial Guide"), 73; *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369-1370 (Fed. Cir. 2016); *Henny Penny Corporation v. Frymaster LLC*, 938 F.3d 1324, 1330-1331 (Fed. Cir. 2019). It would be fundamentally unfair to consider this new theory, at least because the rules bar

Patent Owner from introducing any new evidence in response. Trial Guide, 73. Petitioner chose what grounds and evidence to advance in its Petition and should not be permitted to amend its Petition on Reply.

If the Board were to reach the merits of Petitioner's improper new theory, it should be rejected for this simple reason: Ishiyama discloses communication with a correspondent host and never once suggests that it could possibly be a security gateway. Ishiyama is aware that RFC 2401 discloses two possible endpoints. Ex. 1004 [Ishiyama] 0014 (7:46-49). But Ishiyama states that its endpoint is a correspondent host, not a security gateway, in each of the multiple embodiments that are disclosed. Ishiyama references the "correspondent host" endpoint forty-two times. Ishiyama never once mentions a "security gateway." Accordingly, a POSITA would not have understood Ishiyama to include a security gateway or suggest a security gateway.

B. Petitioner's Misleading Argument That The Care-Of Address Referred To As The "Gateway Address" Of The Mobile Terminal In Ishiyama Is Actually A Security Gateway Should Be Rejected

The Reply also argues, for the first time,[3] that Ishiyama's characterization of mobile host 2's Care-of address as being its "gateway address" is actually a disclosure that correspondent host 3 is a security gateway. Reply, 9.

Petitioner misleadingly cites to Ishiyama as ostensibly disclosing such a security gateway by truncating the quotation at Ishiyama 8:1-6 to remove the portion which explains that the care-of gateway address is that of "the **mobile computer 2** of FIG. 3." See Reply, 9; Ex. 1004 [Ishiyama] 0014 (8:1-6) (emph. added). Mobile computer 2 is indisputably **not** a security gateway and Petitioner has never suggested that it is.

Petitioner further asserts that "Ishiyama also describes 'CoA updating,' where the 'correspondent host 3' updates a 'gateway address' when a mobile terminal moves to another network. *Id.*, 8:66-9:10." Reply, 11. The full passage, however, confirms that the referenced "gateway address" is the updated care-of address CoA2 of mobile computer 2 carried in a message that causes the

[3] Petitioner's theory and proffered evidence that the "gateway address" is a security gateway should be rejected as an improper new theory.

correspondent host 3 to update its database for the new endpoint address of mobile computer 2. Ex. 1004 [Ishiyama] 0014-0015 (8:59-9:10).

In sum, Ishiyama's "gateway address" is an address of the mobile computer, not the correspondent host. Furthermore, the gateway address is a network address, not a security gateway. Petitioner's statements that Ishiyama "explicitly states that its host is a gateway" and that "Ishiyama repeatedly refers to its correspondent host as a 'gateway'" are flatly wrong. Reply, 9, 11.

C. None Of Petitioner's Other Miscellaneous Arguments Is Persuasive

Petitioner does not dispute Patent Owner's explanation (see POR, 35-37) that the use of single-address selectors for the security policy databases (SPDs) in Ishiyama means that correspondent host 3 is not a security gateway. Reply, 13. Likewise, Petitioner does not dispute Patent Owner's point (POR, 34) that the use of CN as an inner destination address means that the correspondent host cannot be a security gateway. Reply, 13. Rather than address the merits, Petitioner dismisses these points as "focus[ing] on "narrow embodiments" in Ishiyama. But Petitioner fails to identify any different embodiments in Ishiyama that produce a different result.

Petitioner suggests that a correspondent host and security gateway are interchangeable devices, citing to the declaration of Dr. Rouskas. Reply, 14. Dr.

Rouskas simply recognizes that the same system can sometimes perform different functions, such as a security gateway occasionally functioning as a host when it processes certain commands. Ex. 2009 [Rouskas Decl.] (¶ 70). However, the converse is not true: A host cannot provide a security gateway functionality to receive and forward packets because a host has only a single interface. See POR, 16, n.1 (citing Ex. 2009, ¶70.), Ex. 2009, ¶¶78, 82-83, 110-111. Accordingly, a host such as Ishiyama's correspondent host 3 cannot function as a security gateway.

Petitioner argues that "nothing precludes the [security database] elements" and other elements of Ishiyama "from being used in a common security gateway configuration, such as described by Murakawa." Reply, 10-14.[4] Ishiyama's specification should be interpreted for what it affirmatively teaches as opposed to what it does not "preclude." *See In re Smith International, Inc.*, 871 F.3d 1375, 1382-83 (Fed. Cir. 2017) ("The correct inquiry . . . is not whether the specification

[4] Petitioner cites to RFC 2401 and Dr. Rouskas's testimony to show that security databases are used in IPSec. Reply, 13. That misses the mark. Petitioner fails to explain how the specific security databases disclosed in Ishiyama would or could be modified to incorporate the security gateway structure of Murakawa.

proscribes or precludes some broad reading . . . It is an interpretation that corresponds with what and how the inventor describes his invention in the specification.'") (cite omitted). Ishiyama does not disclose or suggest a security gateway, nor does it suggest incorporating its security databases into a security gateway, and it certainly does not disclose how its security databases could be modified and incorporated into a security gateway.

V. PETITIONER FAILS TO DEMONSTRATE HOW ISHIYAMA AND MURAKAWA COULD BE COMBINED

Petitioner asserts that "[t]he Petition explicitly presents how Ishiyama and Murakawa would be combined." Reply, 14.[5] This is not the case. Petitioner's Reply simply does not address the defect that Patent Owner pointed out repeatedly in its Response, which is that the Petition fails to explain **how** Ishiyama and Murakawa are combined and **what is the operation** of the resulting system. See

[5] Petitioner's knack for jumping between arguments makes it impossible to discern its operating theory. For example, the Petitioner states that the Board was correct that Murakawa provides the claimed "security gateway." Reply, 10. Yet on the previous page Petitioner takes a contrary position in stating that Ishiyama provides the "security gateway." Reply, 9.

POR at 51-52 (citing to *Personal Webs. Techs., LLC v Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017)).

Petitioner asserts that "a POSA would have easily implemented Ishiyama's address changing functionality with Murakawa's security gateway," Reply, 15, and "Ishiyama's address changing functionality would have been incorporated into security gateways . . . such as the one depicted in Murakawa." Reply, 16-17. However, Petitioner never goes on to explain the combination and how it works. If the combination was so "eas[]y," surely Petitioner could provide a basic description of how Ishiyama and Murakawa are combined and how the resulting system operates. To this day, Petitioner never has.

As best as can be discerned, Petitioner appears to be relying on a combination in which Murakawa's security gateway 103 ("security gateway") and PC 106 ("other terminal") fill the gaps of Ishiyama. But critically, Petitioner never explains how they would be combined with Ishiyama or how Ishiyama's address changing functionality would operate within the contours of Murakawa's system. For example, Petitioner fails to explain what modifications to Ishiyama's Security Policy Databases (SPDs) and Security Association Databases (SADBs) (see Figs. 8-9 of Ishiyama, Ex. 1004) would be required for Ishiyama to work with a security gateway 103 as the opposing endpoint instead of correspondent host 3. Patent Owner made this very point in its POR (at 53) and Petitioner provides no response other than Dr. Goldschlag's *ipse dixit* conclusion that "Ishiyama's description and use of an SAD and SPD does not preclude Ishiyama from being combined with Murakawa to teach" the claimed invention. See Ex. 1022 [Goldschlag Reply Decl.] ¶56 (cited by Reply, 17). That falls far short of explaining of how the teachings could be combined so as to arrive at the claimed invention.

VI. THE PETITION DID NOT SHOW CLAIMS 3 AND 5 TO BE UNPATENTABLE

A. Claims 3 And 5 Were Challenged Under Ground 2 And Petitioner Cannot Amend Its Petition To Challenge Them Under Ground 1

Claims 3 and 5 recite that a "reply message" is sent back from the secure gateway in response to the mobile terminal's "request message" for the address definition of the secure connection to be redefined. As presented in the Petition and set forth in the Institution Decision, review of claims 3 and 5 was instituted under Ground 2 (Ishiyama, Murakawa, and Ahonen). Paper 10 [Institution] 42.

Petitioner's submission of new evidence and its effort to mount a new challenge to claims 3 and 5 under Ground 1 should be rejected. See Reply, 19. The Petitioner may not use the reply to present new grounds not found in the petition.

Furthermore, Petitioner already expressly conceded that claims 3 and 5 were not unpatentable under Ground 1 and cannot reverse course now. When the Petition was filed, Petitioner and its expert both specifically conceded that the combination of Ishiyama and Murakawa does not teach the "reply message" recited in claims 3 and 5:

- "Ishiyama and Murakawa, however, do not explicitly describe this reply message . . . [T]he combination does not explicitly describe a reply message being transmitted from a security gateway to a mobile terminal." Pet., 55.
- "That is, after an address update request message has been sent from a mobile terminal, Ishiyama and Murakawa do not describe how a mobile terminal would be informed that the address was successfully updated before initiating communications from the new address. Goldschlag Decl., ¶123." Pet., 55-56.

B. Claims 3 And 5 Are Not Unpatentable Under Ground 2 Because Ahonen Fails To Teach Or Suggest The Recited "Reply Message"

Petitioner explains that it "relies on Ahonen . . . for the teaching of reply messages in the context of address updates." Reply, 20. Petitioner argues that Ahonen's "ACK" acknowledgement is a reply to a mobile terminal's request to change the address endpoint of a secure connection between the mobile terminal and the security gateway, as claimed.

Petitioner's argument fails for two reasons. First, Ahonen discloses that the mobile terminal submits a request for permission to use an SA defining a secure connection between the mobile terminal and **the correspondent host,** not between the mobile terminal and **security gateway as claimed**. Ex. 1006 [Ahonen] 0010

(Col. 9:23-25); 0010 (Col. 10:21-27: "After the mobile host 1 has received the 'ACK' message . . . the mobile host 1 can begin to send application traffic to the correspondent host 4 by utilizing the **acknowledged phase 2 SA (between the mobile host 1 and the correspondent host 4.")**) [all emph. added].

Petitioner is correct that the request ("control authorization certificate") is received at the firewall/security gateway (Reply, 21), but misses the point, which is that Ahonen's request is for a secure connection between the mobile terminal and correspondent host. In sum, the secure connection in Ahonen that is requested and acknowledged is between a mobile terminal and a correspondent host, not between a mobile terminal and a security gateway as claimed.

Second, Ahonen's ACK message replies to a request by the mobile terminal to use a specific SA, not a request to change the address of a secure connection as claimed. Ahonen's mobile terminal submits a request for "this mobile host 1" to use a specific SA defined by the "ISAKMP cookies," "IPsec protocol ID," and the "SPI number." Ex. 1006 [Ahonen] 0010 (9:30-45). The firewall determines if there is a record in the RCDB matching the four input parameters (mobile terminal 1, ISAKMP cookies, IPsec protocol ID, and SPI). If there is a match, then the specific SA can be used for mobile host to correspondent host communications. Ex. 1006

[Ahonen] 0010 (9:50-10:8). Notably, the match is not based on the address of the mobile terminal.[6]

If there is a match, various parameters in the RCDB can be updated, including "the Source and Destination IP addresses . . . if they are changed," the remote control flag and the initial sequence number. Ex. 1006 [Ahonen] 9:62-10:3. There will be no updating of Source and Destination IP addresses if they have not changed. This illustrates that the purpose--and effect--of Ahonen's request is to determine whether a specific SA can be used, not to change the address definition of an SA. Accordingly, Ahonen's response is to a request to use a specific SA, not a request to change the address definition of an SA.

[6] If Ahonen's control authorization certificate were a request to change the address definition of a secure connection, then the RCDB would perform a match comparing the existing address of the mobile terminal to the stored address of the mobile terminal. However, no such comparison is performed. The comparison is based solely on the identity of the mobile terminal and the three parameters that define the requested SA. See Ex. 1006 [Ahonen] 0010 (9:52-61).

VII. CLAIMS 6-8 ARE PATENTABLE OVER THE APPLIED REFERENCES

Each of claims 6-8 includes the limitation of intervening claim 5 of "the security gateway sending back a reply message to the mobile terminal at the second address to confirm the address change." As explained in the POR (63-64, 73), the Petition fails to address the intervening limitation of the reply message for claims 6-8.

The Reply Brief's assertion (at 23) that "[t]he Petition plainly explains how each limitation of claims 6 and 7 are taught by Ishiyama and Murakawa" and "each limitation of claim 8 is taught by Ishiyama, Murakawa, Forslöw" is misleading. Claim 6 is analyzed in the Petition at 50-53, which does not address the recited reply message. Claim 7 is addressed without any reference to the recited reply message. See Petition, 54. Claim 8 is analyzed without regard to the recited reply message. Petition, 61-64.

Petitioner's attempt to redefine its grounds at the reply stage should be rejected. See Reply, 22-26. Petitioner cannot modify its Petition in *ex post facto* fashion to change the challenges to claims 6-8 to new or modified grounds.

Finally, Petitioner states that it would not object to Patent Owner's sur-reply including new evidence and going beyond the page limit to address Petitioner's new grounds on the intervening claims. Reply, 26 n.2. However, Petitioner has no power to waive the Board's rules and Petitioner's improper attempt to add new grounds in its reply is not a good basis for the Board to waive rules. Instead, the Board should honor the goal of IPRs providing a streamlined proceeding and honor the holding of *SAS* by simply discarding the new grounds as outside the scope of the petition.

VIII. CONCLUSION

For the foregoing reasons, the claims should be affirmed.

Respectfully submitted,

/James T. Carmichael/
James T. Carmichael, Reg. No. 45,306
CARMICHAEL IP, PLLC

Date: May 12, 2020

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Sur-Reply to Petitioner's Reply to Patent Owner's Response consists of 5448 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. This paper complies with the type-volume limitation of 5600 words as mandated in the November 2019 Consolidated Trial Guide, 38; see 37 C.F.R. § 42.24(c). In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Respectfully submitted,

/James T. Carmichael/

Date: May 12, 2020

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served by electronic service, by agreement between the parties, on the date below:

PATENT OWNER'S SUR-REPLY TO PETITIONER'S REPLY TO PATENT OWNERS RESPONSE

The names and address of the parties being served are as follows:

Michael D. Specht	mspecht-PTAB@sternekessler.com
Daniel S. Block	dblock-PTAB@sternekessler.com
Timothy L. Tang	ttang-PTAB@sternekessler.com
	PTAB@sternekessler.com

Respectfully submitted,

/James T. Carmichael/

Date: May 12, 2020