IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

NETWORK PROTECTION SCIENCES, LLC, Plaintiff, v. FORTINET, INC., Defendant. _______________________/	No. C 12-01106 WHA **CLAIM CONSTRUCTION ORDER**

INTRODUCTION

In this patent infringement action involving network firewalls, the parties seek construction of six phrases found in the asserted patent. On December 21, 2012, a tentative claim construction order was issued, and the parties were invited to file five-page critiques of the constructions therein. After consideration of the supplemental briefing, final constructions of the six phrases are set forth below.

STATEMENT

The technology described in United States Patent No. 5,623,601 dates to 1994. Although the modern internet was still unknown to large sections of the general public at the time, networked computing had been around for decades. Computer viruses and other network security threats were already a problem of substantial concern. Computer firewalls — network barriers that analyze packets of information to determine whether they should be let through —

were a relatively recent response to these threats. The technology at issue in this action relates to firewall technology intended to improve network security and user convenience.

Plaintiff Network Protection Sciences ("NPS") is asserting 54 of the 59 claims in the '601 patent against defendant Fortinet, Inc. The parties seek construction of six phrases appearing in this patent. This claim construction order follows a tentative claim construction order, oral argument, and subsequent briefing by defendant Fortinet (NPS submitted to the constructions in the tentative claim construction order without further critique (Dkt. No. 188)).

ANALYSIS

1. CLAIM CONSTRUCTION LEGAL STANDARD.

Claim construction is from the perspective of one of ordinary skill in the pertinent art at the time the patent was filed. *Chamberlain Group, Inc. v. Lear Corp.*, 516 F.3d 1331, 1335 (Fed. Cir. 2008). While claim terms "are generally given their ordinary and customary meaning," the "claims themselves provide substantial guidance as to the meaning of particular claim terms." As such, other claims of the patent can be "valuable sources of enlightenment as to the meaning of a claim term."

Critically, a patent's specification "is always highly relevant to the claim construction analysis." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–15 (Fed. Cir. 2005) (en banc) (internal quotations omitted). Indeed, claims "must be read in view of the specification, of which they are a part." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996). Finally, courts also should consider the patent's prosecution history, which "can often inform the meaning of the claim language by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be." These components of the intrinsic record are the primary resources in properly construing claim terms. Although courts have discretion to consider extrinsic evidence, including dictionaries, scientific treatises, and testimony from experts and inventors, such evidence is "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at 1317–18 (internal quotations omitted).

While this order acknowledges that the parties have a right to the construction of all disputed and litigated claim terms by the time the jury instructions are settled, the Court will reserve the authority, on its own motion, to modify the constructions in this order if further evidence — intrinsic or extrinsic — warrants such a modification. Given that claim construction is not a purely legal matter, but is (as the Supreme Court describes it) a "mongrel practice" with "evidentiary underpinnings," it is entirely appropriate for the Court to adjust its construction of claims prior to instructing the jury if the evidence compels an alternative construction, or if one side or the other advances a spin on the words that is unwarranted. *Markman*, 517 U.S. at 378, 390. The parties should be aware, however, that they are not invited to ask for reconsideration of the constructions herein. Motions for reconsideration may be made only in strict accordance with the rules of procedure, if at all.

2. THE '601 PATENT.

The '601 Patent, entitled "Apparatus and Method for Providing a Secure Gateway for Communication and Data Exchanges Between Networks," was filed on November 21, 1994, and issued on April 22, 1997. Milkway Networks Corporation is the assignee, and plaintiff is Milkway's successor-in-interest. In 2011, Fortinet filed a request for reexamination, and in May, 2012 the USPTO issued a reexamination certificate for the patent confirming all claims (1–41) and adding new claims (42–59).

In this action, NPS is asserting 54 of the 59 claims in the '601 patent, including both method and apparatus claims. The six claim terms for which the parties seek constructions can be found, *inter alia*, in claims 1, 10, and 11 (reproduced below with the relevant claim terms italicized).

Claim 1 covers the following method (col. 14:11–42):

> 1. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:
>
> (a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to the host, but encapulating [*sic*] the packets with a hardware destination address that matches a device address of the gateway;

(b) *accepting at the gateway* communications packets from either network that are encapsulated with a hardware destination address which matches the device address of the gateway;

(c) determining at the gateway whether there is a *process bound to a destination port number* of an accepted communications packet;

(d) establishing *transparently* at the gateway a first communications *session* with a source address/source port of the accepted communications packet if there is a *process bound to the destination port number*, else dropping the packet;

(e) establishing *transparently* at the gateway a second communications *session* with a destination address/destination port of the accepted communications packet if a first communications *session* is established; and

(f) *transparently* moving data associated with each subsequent communications packet between the respective first and second communications *sessions*, whereby the first *session* communicates with the source and the second *session* communicates with the destination using the data moved between the first and second *sessions*.

Claim 10 covers the following method (cols. 15:45–16:14):

10. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:

(a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to the host, but encapulating [*sic*] the packets with a hardware destination address that matches a device address of the gateway;

(b) accepting from either network all TCP/IP packets that are encapsulated with a hardware destination address which matches the device address of the gateway;

(c) determining whether there is a *proxy process* bound to a port for serving a destination port number of an accepted TCP/IP packet;

(d) establishing a first communications *session* with a source address/source port number of the accepted TCP/IP packet if there is [*sic*] *proxy process* bound to the port for serving the destination port number, else dropping the packet;

(e) determining if the source address/source port number of the accepted packet is permitted to communicate with a destination address/destination port number of the

> accepted packet by referencing a rule base, and dropping the packet if a permission rule cannot be located;
>
> (f) establishing a second communications *session* with the destination address/destination port number of the accepted TCP/IP packet if a first communications *session* is established and the permission rule is located; and
>
> (g) *transparently* moving data associated with each subsequent TCP/IP packet between the respective first and second communications *sessions*, whereby the first *session* communicates with the source and the *second* session communicates with the destination using the data moved between the first and second *sessions*.

Dependent claim 11 covers the following method (col. 16:15–23):

> 11. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10 wherein the step of determining involves checking a table to determine if a custom *proxy process* is *bound to the destination port number*, and passing the packet to a *generic proxy process* if a custom *proxy process is not bound to the destination port number*, the *generic proxy process* being executed to establish the first and second communications *sessions* and to move the data between the first and second communications *sessions*.

The patent addresses a basic concern created by the existence of public and private computer networks. Private networks, such as single corporation's intranet, are relatively secure and often store trade secret and confidential information that must be shielded from public exposure. Public networks, such as the internet, are accessible to anyone with the right hardware and software, and as a consequence attract sabotage, vandalism, and espionage. When a private network connects to a public network, it becomes exposed to these threats. To deal with the problem, secure gateways are installed between the networks to serve as "firewalls" (col. 1:23–40).

At the time of the invention, firewalls suffered from known disadvantages that compromised their security or inconvenienced users. One firewall technology in the prior art was the "packet filter." Packet filters were (and are) host-based applications that permitted certain kinds of communications over predefined ports and used pre-defined rule sets to determine what information to let through. Because an operating system such as UNIX running TCP/IP (the communication protocol for the internet) could have 64K communication ports, it was considered impractical to maintain a comprehensive rule base (col. 2:35–45).

Another firewall technology, “dual homed gateways,” blocked direct traffic and required the public and private networks to each communicate with the gateway. When implemented at the application level, users could (and can) only access specific public services allowed by the gateway. These application level firewalls, however, were inefficient because they generally required the user to execute time-consuming extra operations or to use specially-adapted network-service programs (col. 3:4–22). Also, application level firewalls required application interfaces for each public network service and did not support applications using dynamic port allocations assigned in real time (col. 3:48–52).

The claimed invention allegedly overcame these problems by modifying a secure gateway station to accept all IP packets with a certain encapsulation. The invention provided for communication sessions to be initiated between (i) the source network (the network sending the packet) and (ii) the destination network (the network receiving the packet). The “payload” data in the packet were then passed between the two sessions. The new process was more efficient for the user because from the user’s perspective the information was passed as if no gateway existed. The invention also provided for a generic proxy process to handle data such that the gateway could use all 64K ports available on a UNIX operating system and could support dynamic port allocation (cols. 4:17–5:55).

A. “Session”

The parties dispute the term “session.” Both provide constructions, but NPS argues that “session” is a term of art that preferably should be given its ordinary meaning. The parties’ proposed constructions are provided below:

NPS' PROPOSED CONSTRUCTION	FORTINET'S PROPOSED CONSTRUCTION
Plain and ordinary meaning; or A connection between two functional units, such as two terminals, stations, or computers, that allows them to communicate for a period of time or a logical association that is established and maintained between two functional units that allows them to communicate.	The application level network gateway and source maintain a connection and transfer information, or the application level network gateway and destination maintain a connection and transfer information.

This order concludes that the plain and ordinary meaning of the term "session" should govern, as understood by one of ordinary skill in the art in 1994.

NPS' proposed alternative construction for "session" is turgid and unhelpful. Its proposal to use the ordinary meaning fares better. NPS does not provide much explanation for its argument that the term should be given its ordinary meaning. Nevertheless, it was a straightforward term in 1994 (and today).

Fortinet's only challenge to using the ordinary meaning of the term "session" is that the patent "always" referred to a session as including the transfer of information. Fortinet's assertion is incorrect. Information *could* be transferred during a session, for example by a proxy process or by the kernel (the program at the core of the computer operating system that supported programs running at the application level). The specification also disclosed a situation where a proxy process handling communications would not transfer information. The proxy process could determine that a session had not ended and could wait for data packets to arrive (col. 11:56–65). If a proxy process could wait for data to arrive during an active session but without transferring data, it is clear that a session did not necessarily require information transfer.

This order concludes that the plain and ordinary meaning of the term "session" should govern (subject to a possible refinement after the trial evidence is heard).

B. "Proxy process"

The parties dispute the term "proxy process." The parties' proposed constructions are as follows:

NPS' PROPOSED CONSTRUCTION	FORTINET'S PROPOSED CONSTRUCTION
An application layer process adapted to handle a respective service. or (at oral argument): An application layer process adapted to handle communications across a gateway for a respective service.	A program running on an application level network gateway that initiates the first session and second session, and relays "the data portion of each packet" between the sessions. or (in its critique): an application layer process that relays the 'data portion of each packet' between the first and second communications sessions.

This order finds that the term should be construed as: "an application layer process adapted to handle communications for a network service."

The term "proxy" was defined in the patent specification. To wit:

> When the gateway station 14 is initialized, a system configuration file is examined to determine what network services are to be supported by the gateway station 14. In order to maximize performance efficiency of the gateway station 14, commonly used services are supported by processes adapted to most efficiently handle communications for each respective service. These processes are called "proxies."

(Col. 9:47–54.) NPS' proposed constructions are reworded versions of this definition.

Fortinet contends in its claim construction critique that this text does not evince a clear intention to define the term "proxy." Based on the plain language, this order disagrees. Similarly, Fortinet contends that this text does not purport to define claim language, only a preferred embodiment. Although this language does appear in relation to Figure 6 in the patent, there is no express indication that the patentee intended to limit this definition to Figure 6 alone, or intended to vary the definition elsewhere in the patent.

Fortinet also asserts that it is improper to rely on an isolated passage of the specification in support of a broad construction. Fortinet's attempt to define the patent differently than it was defined by the patentee himself is unpersuasive.

Fortinet asserts that NPS' proposed construction is an attempt to scrub the patent of its reliance on a "proxy concept," and that the term should be construed to require a process that "actually acts as a proxy." At oral argument, Fortinet explained that the patent should be viewed through a particular technological lens — what Fortinet refers to as a "proxy everything" environment. This is an attempt to limit the scope of the claims generally by creating a limiting context. Otherwise, Fortinet contends, NPS' definition could be read to include any process, even processes that are not proxies, or "any communications service."

Fortinet's desire to ignore the definition in the specification is improper. "It is a well-established axiom in patent law that a patentee is free to be his or her own lexicographer, and thus may use terms in a manner contrary to or inconsistent with one or more of their ordinary meanings." *Hormone Research Found., Inc. v. Genentech, Inc.*, 904 F.2d 1558, 1563 (Fed. Cir. 1990) (citation omitted). "When a patentee explicitly defines a claim term in the patent specification, the patentee's definition controls." *Martek Biosciences Corp. v. Nutrinova, Inc.*, 579 F.3d 1363, 1380 (Fed. Cir. 2009).

Aside from this general principle of patent claim construction, the specific limitations requested by Fortinet are unwarranted. In its claim construction briefing, Fortinet asserts that the term proxy process should be limited to include (i) the concept of relaying a data packet between communication sessions, and (ii) the concept that the proxy process initiated the communication sessions. Fortinet's critique of the tentative claim construction order repeats this argument, stating that "[f]undamentally, any 'proxy' necessarily breaks a single communications session into two sessions and relays data between them." Fortinet insists that the term "'proxy process' ought to incorporate — somewhere — the concept of a proxy" as Fortinet understands the term. Yet, Fortinet fails to address how its proposed construction addresses situations in the patent where a proxy process deviates from Fortinet's proposed limitations.

NPS agrees that a proxy process can relay data, but does not agree that it should always be so limited. In support, NPS cites examples in the specification where a proxy process did something else, such as verifying an IP address. Fortinet's limitation, therefore, goes too far.

In its critique, Fortinet offers a compromise construction: "an application layer process that relays the 'data portion of each packet' between the first and second communications sessions." Fortinet's compromise remains too restrictive because a proxy process in the patent does not necessarily relay data between communications sessions. Fortinet's assertion that "a proxy *always relays and must necessarily relay* the data portions of packets *between two communications sessions*" (Dkt. No. 187 at 3 (emphasis added)) is incorrect. This is evident from claim 18, which discloses a situation where a proxy process relays data from the kernel to another proxy process, to wit: "whereby the TCP/IP packet is passed by a modified kernel of an operating system of the secure gateway to the proxy process which extracts the data from the packet and passes the data from a [*sic*] one of the . . . communications sessions to a proxy process . . . [which] executes data screening algorithms" (col. 17:31–38).

NPS concedes that a proxy process can relay data, but the patent discloses situations where the data is relayed between communications sessions, between the kernel and a proxy process, and between proxy processes. The Court's construction — "an application layer process adapted to handle communications for a network service" — remains the most suitable because the various forms of data relay and other disclosed proxy process activities are within the general scope of "handling communications."

As for whether the proxy process initiated the communication session, Fortinet concedes that NPS cites examples from the specification where the gateway or kernel initiated the communications. Fortinet contends that these examples are ambiguous. This order disagrees. In particular, Figure 6, which was a "flow diagram of . . . TCP routing by a modified UNIX kernel in accordance with the invention" (col. 6:65–67), showed that the kernel started a session with a source prior to delivering a packet to a proxy process. The fact that elsewhere in the patent the proxy process initiated the communication session only demonstrates that both ideas were disclosed.

Another objection by Fortinet in its papers points out a flaw in NPS' original proposed construction. A close comparison of the definition in the specification and NPS' proposed construction reveals that NPS has omitted the concept of handling communications. This omission unjustifiably broadens the scope of the claim language and is easily corrected. At oral argument, NPS conceded this point by offering compromise construction that included the concept of communications. In order to align the construction with the definition, this order specifies that the proxy process handles "communications for a network service."

The full construction of "proxy process" therefore shall remain: "an application layer process adapted to handle communications for a network service." Fortinet's concern that this construction could be warped to encompass "any communications process" is noted. This order reserves the authority to modify the construction at a later time if necessary.

C. "Generic proxy process"

During briefing and oral argument, the parties modified and narrowed their differences over this term, but they still dispute the term "generic" as it modifies the term "proxy process." The parties' current proposed constructions are shown below:

NPS' PROPOSED CONSTRUCTION	FORTINET'S PROPOSED CONSTRUCTION
A process which can handle a service for which a dedicated or custom proxy process is not running. or (at oral argument): A proxy process which can handle a service for which a dedicated custom proxy process is not running. or: A "proxy process" that serves any service not already served by a dedicated or "custom" proxy process.	A proxy process that serves any application not already served by a dedicated custom proxy process.

This order construes "generic proxy process" as "a proxy process which can handle communications for a network service for which a dedicated or custom proxy process is not running."

Aside from the underlying disagreement over "proxy process," one aspect of the parties' dispute over this term is whether the terms "dedicated" and "custom" should be listed in the conjunctive or the disjunctive. The specification referred to the generic proxy process operating

United States District Court
For the Northern District of California

wherever there was not a "dedicated proxy process" (col. 5:48–52). It is also clear from the specification that the inventor anticipated that a generic proxy process could support a network service until a new, custom proxy process was written (col. 12:52–55). Thus, the invention conceived of at least three proxy scenarios: a dedicated proxy, a generic proxy, and a custom proxy that displaced a generic proxy already in use. Fortinet's construction in the conjunctive cannot accommodate all three possibilities and is therefore too narrow. This order will use the disjunctive phrasing "dedicated or custom."

The other significant distinction between the proposed constructions lies in the gap between "handle a service" and "serves any application." Here, Fortinet's proposed construction strays too far afield from the definition of proxy provided by the inventor, and the phrase "serves any application" is ambiguous.

A "generic proxy process" was a specific type of "proxy process." Once again, NPS' construction strays from the definition of "proxy process" in the specification. For clarity and consistency, this order will rely on the inventor's definition.

In sum, a "generic proxy process" shall be construed to mean "a proxy process which can handle communications for a network service for which a dedicated or custom proxy process is not running."

D. "Process bound to a destination port number"

During briefing, both parties modified their proposed constructions of this term, but the parties still dispute "process bound to a destination port number." The parties' latest proposed constructions are:

NPS' PROPOSED CONSTRUCTION	FORTINET'S PROPOSED CONSTRUCTION
Plain and ordinary meaning; or Process assigned or linked to a destination port number.	Proxy process that is bound to the port on the gateway that matches the destination port number of the incoming packets. or: Proxy process bound to a destination port.

This order construes "process bound to a destination port number" as meaning a "process assigned to a destination port number."

The parties do not appear to dispute the "destination port number" component of the term, and the parties did not address the issue in their briefs or at oral argument. Fortinet nevertheless provides a proposed construction for this element. Fortinet's construction defines "destination port number" as "the port on the gateway that matches the destination port number of the incoming packets." Compared with a plain meaning construction, Fortinet's proposal for this segment is wordy and potentially confusing. Fortinet also does not explain why explication of "destination port number" is necessary.

The parties' dispute involves two issues. *First*, they dispute whether "process" must be construed to refer to a "proxy process." This is the focus of the parties' dispute over this term, both in the briefing and at oral argument. Here, Fortinet again offers its unsubstantiated contention that the patent taught a "proxy everything" environment. Fortinet further contends that the intrinsic evidence shows that "process bound" always meant a "proxy process."

What Fortinet's contentions do not account for is how the term was actually used in the claims. The disputed term appeared in claim 1 in the following clauses:

> (c) determing at the gateway whether there is a ***process*** *bound to a destination port number* of an accepted communications packet;
>
> (d) establishing transparently at the gateway a first communications session with a source address/source port of the accepted communications packet if there is a ***process*** *bound to the destination port number*, else dropping the packet;

(Col. 14:23–29 (emphasis added).) In claim 10, the term was used differently:

> (c) determining whether there is a ***proxy process*** *bound to a port for serving a destination port number* of an accepted TCP/IP packet;
>
> (d) establishing a first communications session with a source address/source port number of the accepted TCP/IP packet if there is [*sic*] ***proxy process*** *bound to the port for serving the destination port number*, else dropping the packet;

(Col. 15:56–64 (emphasis added).) In claim 11, there was another variation.

> 11. A method . . . as claimed in claim 10 wherein the step of determining involves checking a table to determine if a ***custom proxy process*** *is bound to the destination port number*, and

> passing the packet to a generic proxy process if a ***custom proxy process*** *is not bound to the destination port number* . . . .

(Col. 16:15–20 (emphasis added).) The reader will note the progression: a "process" was claimed in claim 1, but a "proxy process" and a *specific type* of "proxy process" appeared in claims 10 and 11, respectively. It seems clear that the drafter intended to refer to different types of processes being bound. Fortinet's construction of the disputed term to mean "proxy process" in claim one would therefore require reading a limitation from the specification into the claims, or limiting a broader claim based on subsequent narrower claims. This would be improper. Fortinet's construction would also render the language in claims 10 and 11 that specifies a "proxy process" superfluous.

Second, the parties dispute the meaning of the word "bound." Fortinet asserts that bound should be understood to refer specifically to the UNIX "bind" command but does not propose to include that limitation in the construction. Instead, Fortinet asserts that a POSA would have considered the ordinary meaning of the term bound to mean the bind command.

It is useful to note at this point that Fortinet's assumption of a UNIX environment is faulty. It is true that the patent used UNIX to describe an embodiment of the patent (*see* cols. 9:41–10:24). However, the claims of the patent were not limited to the UNIX operating system. For example, claim 19 described an apparatus that included "*an operating system* executable by the gateway station, a kernel of the operating system having been modified . . ." (col:17:41–50 (emphasis added)). Claim 20, which was dependent on claim 19, covered an apparatus "wherein the operating system [was] a Unix operating system" (col. 18:9–12).

NPS also wishes to use the ordinary meaning of the term "bound," but disagrees that it must include the UNIX bind command. NPS offers "assigned or linked" as an alternative meaning for "bound." NPS cites several places in the specification where the term "assigned" is used in relation to the concept of something being "bound," but does not cite any support in the specification for "linked." The use of the term "assigned" to explain "bound" is evident. "Linked" is not.

Upon review of Fortinet's critique, it remains clear that only the word "bound" in the disputed term requires a construction. Helpfully, the patent itself provided a definition:

> On system initialization, any proxy given operating rights by the system administrator is said to "bind" to the port to which the proxy has been assigned. Thereafter, the process is said to be "bound" to the port.

(Col. 9:54–57.) Fortinet argues that this was not a definition, but rather a factual description of a series of events: the system initialized, and then a process assigned to a port was subsequently bound in the sense of the UNIX "bind" command. This reading is not justified from the plain language of the patent, and is premised on Fortinet's unduly narrow assumption that the patent required a UNIX environment.

In its critique, Fortinet argues that the above quote from column 9 of the patent requires that the term bound include the concept of "operating rights." Fortinet thus proposes "assigned to and given operating rights with respect to a specific communications port" as an alternative construction for bound. This construction is rejected. Column 9 also states "[w]hen the gateway station 14 is initialized, the generic proxy *binds* to port 59813, *provided that the systems administrator has given it operating rights to do so*" (col 9:61–64 (emphasis added)). Fortinet's new construction renders the final clause in this sentence superfluous.

Accordingly, this order retains the tentative construction: "process bound to a destination port number" should be construed as meaning a "process assigned to a destination port number."

E. "Transparently"

The parties dispute the term "transparently." The parties' proposed constructions are shown below:

NPS' PROPOSED CONSTRUCTION	FORTINET'S PROPOSED CONSTRUCTION
Such that clients on networks can run network service applications without extra procedures or modifications to accomplish communications across a gateway.	Appearing to the initiator to be one direct communications session.

This order adopts Fortinet's proposed construction of "transparently": "appearing to the initiator to be one direct communications session." Fortinet cites multiple instances in the patent specification and in the declaration of NPS' expert during reexamination where "transparently" was defined in this manner or explained in terms of whether the communications session appears to be direct.

NPS objects on several grounds, none of which are persuasive. *First*, NPS argues that this construction is improper because it defines the term with a description of the subjective result of the claimed method. NPS cites *West v. Quality Gold, Inc.*, No. 10-3124, slip op. at 9–10 (N.D. Cal. Sept. 16, 2011) (Judge Jeremy Fogel), for the proposition that claims should not be defined by the subjective opinion of an individual practicing an invention. NPS's reliance on *West* is misplaced. NPS conflates subjective opinion with a subjective experience of an objective fact. Unlike the phrase "pleasing appearance" in *West*, "transparency" in Fortinet's proposed construction does not require a subjective evaluation. Whether a communication session appears to be direct is only based on whether there is an objectively perceptible intermediary. An intermediary either appears and is perceived by the client, or it does not. This does not require a subjective opinion.

Second, NPS asserts that the patent specification stated that "communications are said to be transparent because the client . . . does not have to run extra procedures or modify the network source code." NPS' paraphrase misstates the patent language. The full section cited by NPS stated:

> The apparatus in accordance with the invention is, however, configured to provide a transparent interface between the interconnected networks so that clients on either network can run standard network service applications transparently without extra procedures, or modifications to accomplish communications across the secure gateway.

(Col. 6:28–34.) NPS' interpretation of this passage improperly turns the last 12 words into an explanation of the word "transparently." The passage did not state that the network service applications were transparent *because* they were run without extra procedures or modifications. Rather, transparency was one of three distinct characteristics of network service applications in the patented invention. Further, Fortinet's proposed construction allows this passage to be read without rendering the last 12 words in the sentence redundant.

Third, NPS points out that during reexamination, Fortinet's proposed definition of transparently was something more akin to NPS' current construction, and that Fortinet has since changed its tune. At the time, Fortinet was pushing to define transparency as not requiring a user login. This is similar to NPS' current proposal, which references "extra procedures" that NPS argues applied to user logins.

Despite this similarity, Fortinet's prior position is materially different from NPS' current construction. NPS's construction not only references extra procedures, it also references "modifications." Fortinet's prior position and NPS' current position are thus not directly comparable. The fact that Fortinet previously relied on a materially different construction casts doubt over Fortinet's current position, but it does not help NPS in equal measure. Nor is there any basis to deem Fortinet estopped from advancing a different position in this proceeding.

At oral argument, NPS' counsel stated they would accept the same definition of transparently that Fortinet advanced during reexamination. However, the record in this action did not contain adequate briefing on that construction. Based on the available evidence, the tentative claim construction order adopted Fortinet's proposal for "transparently" — "appearing to the initiator to be one direct communications session" — and invited the parties to address the issue of Fortinet's contention at reexamination in their critiques.

Both parties agree with the tentative construction in their critiques. This order holds that no modification is necessary.

F. "Accepting at the gateway"

The parties dispute the term "accepting at the gateway." The parties' proposed constructions are provided below:

United States District Court
For the Northern District of California

NPS' PROPOSED CONSTRUCTION	FORTINET'S PROPOSED CONSTRUCTION
Allowing received packets to be processed by the gateway even though the packets designate an IP destination address other than that of the gateway. or (at oral argument): Allowing received packets to be processed by a gateway with application level security and data screening capability even though the packets designate an IP destination address other than that of the gateway.	Retaining for further evaluation and processing at the application level network gateway.

This order holds that the ordinary meaning of the term to a POSA in 1994 should govern. Although the parties do not recognize their common ground, they agree that "accepting at the gateway" meant "receiving" packets at the gateway instead of rejecting them. This is simply a plain meaning construction of the term, and it is supported in particular by Figure 6 in the patent, which showed the first packet processing step on a UNIX embodiment as "receive data packet." Moreover, at oral argument both parties agreed that a plain meaning construction would be acceptable to them.

This order agrees that a plain language construction charts a better course. Both parties' constructions attempt to read in additional limitations to the claim term, but neither provides an adequate justification for doing so. Fortinet's construction adds the additional element of "retaining for further evaluation." It is clear from the claim language and from Figure 6 of the patent, however, that the disputed term only referred to the first step in the packet processing process, and not to retention after receipt. Fortinet's construction is also ambiguous because it is not clear whether "retaining" refers to receipt at the application level network gateway, or receipt at the gateway before being retained for processing at the application level.

NPS attempts to include a limitation based on the IP destination address of the packet. NPS does not explain why this limitation should be read into the claim and did not address this issue at oral argument. The closest NPS comes to justifying this position is its assertion that language in the patent supports the interpretation that the gateway would accept packets

United States District Court
For the Northern District of California

regardless of their IP address. This is equivalent to arguing that accepting packets regardless of IP destination address was an *implied result* of the other claims. It does not justify adding an additional concept to the definition of the claim term.

Neither party has justified their constructions, and this order shall hold the parties to their common ground at oral argument: the plain meaning of the term to a POSA in 1994 shall govern.

CONCLUSION

The constructions set forth above will apply in this action. The Court reserves the authority, on its own motion, to modify these constructions if further evidence warrants such a modification (but counsel may not move to reconsider them). The Court thanks counsel for their efforts in illuminating the meaning of the foregoing terms.

IT IS SO ORDERED.

Dated: January 14, 2013.

Wm Alsup

WILLIAM ALSUP
UNITED STATES DISTRICT JUDGE