United States District Court,
E.D. Texas, Lufkin Division.

DEEP NINES, INC,
Plaintiff.
v.
McAFEE, INC,
Defendant.

Civil Action No. 9:06-CV-174

March 13, 2008.

Thomas M. Melsheimer, Carl Edward Bruce, Decker A. Cammack, Jennifer Brown Trillsch, Michael Brett Johnson, Thomas Howard Reger, II, Fish & Richardson, Dallas, TX, Andrew Thompson Gorham, Charles Ainsworth, Robert Christopher Bunt, Robert M. Parker, Tyler, TX, Barry Kenneth Shelton, Patrick Scott Richter, Fish & Richardson, Austin, TX, Robert E. Hillman, Fish & Richardson PC, Boston, MA, Timothy Devlin, Fish & Richardson, Wilmington, DE, for Plaintiff.

Martin Edward Rose, Michael Douglas Richardson, Sheetal Chittur Aiyer, Rose Walker, Leane Capps Medford, Elrod, PLLC, Dallas, TX, Danny Lloyd Williams, J Mike Amerson, Jaison Chorikavumkal John, Ruben Singh Bains, Stephen E. Edwards, Terry D. Morgan, Williams Morgan & Amerson, Keith Alan Rutherford, Terril G. Lewis Wong, Cabello Lutsch, Rutherford & Brucculeri, Houston, TX, Eric M. Albritton, Attorney at Law, Longview, TX, J Thad Heartfield, The Heartfield Law Firm, Beaumont, TX, for Defendant.

MEMORANDUM OPINION AND ORDER CONSTRUING CLAIM TERMS OF UNITED STATES PATENT NOS. 7,058,976*;* 6,275,942*;* 7,093,292*; and* 6,742,128

RON CLARK**, District Judge.**

Plaintiff Deep Nines, Inc. filed suit against Defendant McAfee, Inc. claiming infringement of U.S. Patent No. 7,058,976 ("the '976 patent"). McAfee filed counter-claims against Deep Nines, claiming infringement of U.S. Patent Nos. 6,275,942 ("the "2 patent"); 7,093,292 ("the '292 patent"); and 6,742,128 ("the '128 patent"). The court conducted a *Markman* hearing to assist the court in interpreting the meaning of the disputed claim terms. Having carefully considered the patents, the prosecution history, the parties' briefs, and the arguments of counsel, the court now makes the following findings and construes the disputed claim terms as follows. FN1

FN1. The transcript of the hearing contains a number of representations and agreements of the parties and their answers to technical questions from the court, all of which will not be repeated here, but which assisted the court in reaching the conclusions set out in this Order. This Order governs in the event of any conflict between the Order and the court's preliminary analysis at the hearing. The transcript will be cited as

Tr. at p. ----, ll. __.

I. CLAIM CONSTRUCTION STANDARD OF REVIEW

Claim construction is a matter of law. Markman v. Westview Instruments, Inc., 517 U.S. 370, 116 S.Ct. 1384, 134 L.Ed.2d 577 (1996) ("*Markman II*"). "The duty of the trial judge is to determine the meaning of the claims at issue, and to instruct the jury accordingly." Exxon Chem. Patents, Inc. v. Lubrizoil Corp., 64 F.3d 1553, 1555 (Fed.Cir.1995) (citations omitted), *cert. denied,* 518 U.S. 1020, 116 S.Ct. 2554, 135 L.Ed.2d 1073 (1996).

" '[T]he claims of the patent define the invention to which the patentee is entitled the right to exclude.' " Phillips v. AWH Corp., 415 F.3d 1303, 1312 (Fed.Cir.2005) (*en banc*) (citation omitted), *cert. denied,* 546 U.S. 1170, 126 S.Ct. 1332, 164 L.Ed.2d 49 (2006). "Because the patentee is required to 'define precisely what his invention is,' it is 'unjust to the public, as well as an evasion of the law, to construe it in a manner different from the plain import of its terms.' " Phillips, 415 F.3d at 1312 (quoting White v. Dunbar, 119 U.S. 47, 52, 7 S.Ct. 72, 30 L.Ed. 303 (1886)).

The words of a claim are generally given their ordinary and customary meaning. Phillips 415 F.3d at 1312. The "ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." Id. at 1313. Analyzing "how a person of ordinary skill in the art understands a claim term" is the starting point of a proper claim construction. *Id.*

A "person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." Phillips, 415 F.3d at 1313. Where a claim term has a particular meaning in the field of art, the court must examine those sources available to the public to show what a person skilled in the art would have understood the disputed claim language to mean. *Id.* at 1414. Those sources "include 'words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.' " *Id.* (citation omitted).

"[T]he ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words." Id. at 1314. In these instances, a general purpose dictionary may be helpful. *Id.*

However, the Federal Circuit has emphasized the importance of the specification. "[T]he specification 'is always highly relevant to the claim construction analysis. Usually it is dispositive; it is the single best guide to the meaning of a disputed term.' " Phillips, 415 F.3d at 1315 (quoting Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed.Cir.1996)). A court is authorized to review extrinsic evidence, such as dictionaries, inventor testimony, and learned treaties Phillips, 415 F.3d at 1317. However, their use should be limited to edification purposes. Id. at 1319.

The intrinsic evidence, that is, the patent specification, and, if in evidence, the prosecution history, may clarify whether the patentee clearly intended a meaning different from the ordinary meaning, or clearly disavowed the ordinary meaning in favor of some special meaning. *See* Markman v. Westview Instruments, Inc., 52 F.3d 967, 979-80 (Fed.Cir.1995); *aff'd,* 517 U.S. 370, 116 S.Ct. 1384, 134 L.Ed.2d 577 (1996). Claim terms take on their ordinary and accustomed meanings unless the patentee demonstrated "clear intent" to deviate from the ordinary and accustomed meaning of a claim term by redefining the term in the patent specification. Johnson Worldwide Assoc., Inc. v. Zebco Corp., 175 F.3d 985, 990 (Fed.Cir.1999).

The " 'ordinary meaning' of a claim term is its meaning to the ordinary artisan after reading the entire patent." Phillips, 415 F.3d at 1321. However, the patentee may deviate from the plain and ordinary meaning by characterizing the invention in the prosecution history using words or expressions of manifest exclusion or restriction, representing a "clear disavowal" of claim scope. Teleflex, Inc. v. Ficosa N. Am. Corp., 299 F.3d 1313, 1327 (Fed.Cir.2002). It is clear that if the patentee clearly intended to be its own lexicographer, the "inventor's lexicography governs." Phillips, 415 F.3d at 1316.

II. PATENT BACKGROUND AND TECHNOLOGY

A. The '976 patent

The '976 patent describes a system and method for detecting and preventing attacks on a communications network. This system and method consists of a firewall (which will receive and discard data based on a pre-determined set of rules) and an intrusion detection system ("IDS") that will alert the system administrator, block data, and disconnect from the remote source of the hostile attack.

B. The '942, '252, and '128 patents

The "2 patent purports to address a shortcoming of the IDS, namely that the system's response to a particular misuse lacked flexibility to provide a real-time response to the misuse. The "2 patent discloses an active response module ("ARM") architecture for the IDS, which allows the user to use the ARM in a system using any kind of IDS. The ARM includes an arguments component (which specifies the information the IDS misuse engine will need to give to the ARM when the ARM is invoked), an actions component (specifying and causing the ARM's response when the IDS misuse engine invokes it), and the application program interface component (specifying the interface for accessing the network element-like a firewall-with which the ARM will communicate).

The '292 patent addresses another purported shortcoming of the IDS, namely the lack of automatic collection of hacker-related information from multiple computers by a central database and subsequent use of the information to prevent intrusion activity. The '292 patent discloses a plurality of computers with firewalls that collect the information and transmit it over a network to the central server, which then analyzes the information and transmits it back over the network to the computers (in an effort to prevent intrusion activity).

The '128 patent addresses a purported shortcoming of the network threat assessment technology, namely the inability to leverage data from diverse tools (like the IDS and anti-virus programs) in order to collectively detect threats to a network. The '128 patent discloses the collection of network data from these diverse data sources, followed by the aggregation, correlation, and storage of the data in a database. Metadata is generated using the stored data, facilitating access to, and management of, the aggregated data. In order to perform threat assessment profiling, predetermined profiles are compared to the aggregated data. A similar process is used to perform threat assessment prediction.

C. One of Ordinary Skill in the Art

Neither party addressed this important issue in any detail in their briefing or technology synopses.FN2 Based on the patents and their cited references, the tutorials, and the representations of the parties and their experts, the court finds that "one of ordinary skill in the art" covered by the '976, "2, '292, and ' 128 patents is someone with the equivalent of a "four year" degree from an accredited institution (usually denoted in this country as a B.S. degree) with a concentration of courses covering computer programming, networking, and network security. Depending on the institution, the major field of study might be denoted as "electrical engineering," "computer science," or the like. The individual would also have four years of experience in a related field. Additional degrees might substitute for experience, while significant experience in the development and use of computer networks and/or security systems might substitute for formal education. The parties agreed to this definition at the *Markman* hearing. *See* Tr. at p. 17, ll. 3-10.

FN2. McAfee's Reply Brief touches on the issue in a footnote. *See* Doc. # 85 at p. 2, n. 2. According to McAfee, the person of skill in the art has a B.S. degree in computer science, computer engineering, or the equivalent, and at least two years of experience in the analysis, design, and development of network security systems.

III. DISPUTED TERMS IN THE '976, '942, '252, AND '128 PATENTS

With respect to the '976 patent, one of the main disputes between the parties concerns the limitations imposed by the claims on the way in which data flows, and how that data flow is affected by the invention. The first two phrases to be construed are set out below in bold.

1. "A method for detecting attacks on a network, comprising: ... **intercepting in real time the remaining data utilizing the intrusion detection system.**" ' 976 patent**, claims 6 and 12.**

2. "A gateway system for detecting attacks on a network, comprising: ... **an intrusion detection system coupled to the firewall for intercepting in real time remaining data.**" '976 patent**, claim 13.**

For the first phrase, Deep Nines suggests that no construction is required. McAfee proposes "intercepting in real time the remaining data before it gets to the network utilizing the intrusion detection system." As to the second phrase, Deep Nines asserts that the IDS system is "coupled in-line," while McAfee again argues that "intercepting in real time remaining data" means that the remaining data has to be intercepted in real time before it reaches the network. Deep Nines agreed at the hearing that construction of the first phrase would determine the construction of the second, and both parties agreed that the flow of data, rather than some concept of physical "coupling" or location, was the key. Tr. at p. 81, l. 16-p. 85, l. 13.

The real dispute is over McAfee's contention that the IDS should intercept the remaining data "before" it reaches the network FN3 being protected by the IDS. McAfee argues that during prosecution, the applicant disclaimed the interception of data after it reaches the network, in order to distinguish U.S. Patent No. 6,119,236 ("Shipley"). According to the Examiner's Interview Summary, the applicant characterized Shipley's IDS as "inside the network," and went on to state that it "does not block the intrusion in real time ." Interview Summary of 10/12/05, Def. Cl. Const. Br., Ex. 3 [Doc. # 80, p. 1 of 1].FN4

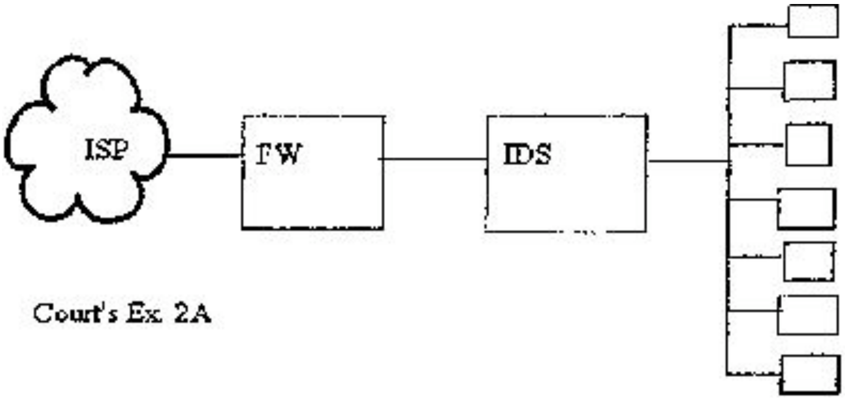
FN3. The parties agree that "network" means "a group of network devices and/or computers interconnected to communicate with each other." *See* Doc. # 99, at p. 4.

FN4. The applicant subsequently amended her independent claims to change "*receiving* the remaining data utilizing the intrusion detection system" to read "*intercepting in real time* the remaining data utilizing the intrusion detection system." Amendment of 10/20/05, Def. Cl. Const. Br., Ex. 2 at 2-5 [Doc. # 80, p. 2 of 12] (emphasis added).

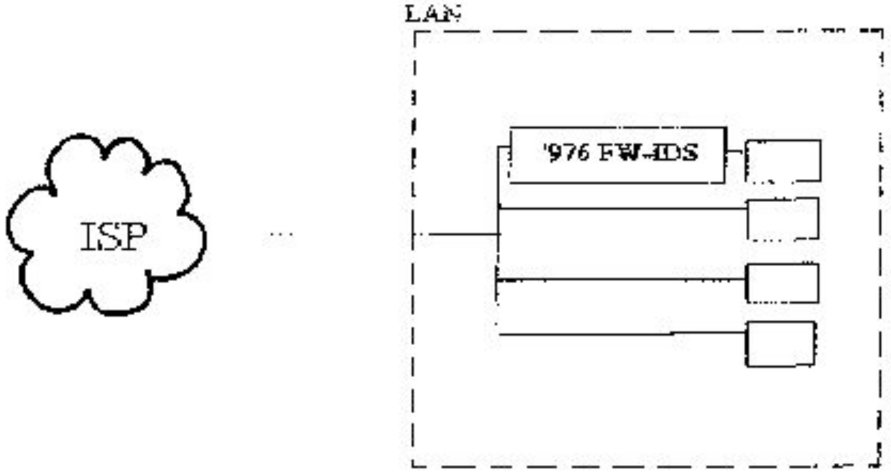
The '976 patent involves the flow of electrons in a hard wire and/or wireless format, and contemplates devices in the network being located in many different places. *See, e.g.,* '976 patent, col. 2, ll. 19-23. Words of physical or spatial relationship, such as "inside" and "outside," may confuse, rather than illuminate, the debate.

Similarly unhelpful is any attempt to define the exact period of "real time," as stated by the Examiner and in the claims of the '976 patent. Even with the speed of today's powerful devices, some scientifically measurable period of time is needed to process data. *See* Tr. at p. 19, l. 13-p. 22, l. 20. It is more useful to examine the disputed phrase from the perspective of data flow and how the invention affects that flow.

The court finds, and the parties agreed, that the flow of data taught in the ' 976 patent can be diagramed as shown in Court's Exs. 1B and 2B. Tr. at p. 68, l. 8-p. 70, l. 3; p. 73, l. 5-l. 24; p. 84, l. 2-p. 85, l. 11; *see also* Court's Ex. 2A and discussion at Tr. at p. 112, l. 20-p. 114, l. 2; p. 115, l. 24-p. 117, l. 16.



Court's Ex. 2A

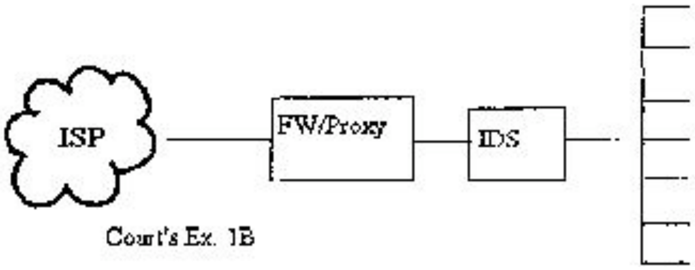


Court's Ex. 3

The data flows from a network or other remote source to a firewall that discards data according to a predetermined set of rules. '976 patent, col. 9, ll. 53-59; *see also* Fig. 1. The "remaining data," being "all of the data that was transmitted by the remote source but not discarded by the application of the firewall rules," FN5 then goes to the IDS where harmful data may be blocked or otherwise acted upon. ' 976 patent, col. 9, ll. 60-61. *See also* Tr. at p. 37, ll. 12-24; p. 68, l. 25-p. 75, l. 17; p. 84, l. 2-p. 85, l. 13. Deep Nines' expert referred to the firewall and the IDS as being "in series." Tr. at p. 36, ll.17-23.

FN5. The parties agreed to this definition. *See* Doc. # 99, at p. 3.

This is contrasted with the flow of data in the Shipley system, where the IDS can "review" the data after it leaves the firewall but can not block it, as diagramed in Court's Ex. 1C.



Court's Ex. 1B

This situation was described as a "wiretap" configuration Tr. at p. 28, ll. 19-25; p. 37, ll. 5-8; p. 69, ll. 10-21.

As noted above, the applicant and the Examiner did distinguish Shipley from the '976 patent by reference to "inside the network." However, the court concludes that the '976 patent and the disputed terms describe the flow of data and how it is acted upon, rather than the physical location of the components. The parties agree that the flow of data described by Shipley is not what is described by this patent. Tr. at 37, ll. 11-24. The court construes these terms as follows:

"Intercepting in real time the remaining data utilizing the intrusion detection system" and **"an intrusion detection system coupled to the firewall for intercepting in real time remaining data"** mean that all of the data that has passed a firewall without being discarded next goes to an intrusion detection system for detecting and acting on attacks before the data is sent to any network device.

3. "Gateway." '976 patent**, claims 6, 12, and 13.**

An exemplar use of this term is seen in claim 12 of the '976 patent, stating in part, with the disputed term in bold:

A method for detecting attacks on a network, comprising:

At a **gateway,** receiving data from a remote source which is destined for a target ...

Deep Nines proposes "an entrance and/or exit to a communications network." McAfee suggests that a gateway "connects two or more different networks." In theory, Deep Nines' proposal might indicate a disagreement over whether some gateways allow data to flow in only one direction; however, as indicated at the hearing, this is not the case. Tr. at p. 88., l. 13-p. 89, l. 10. The real dispute is whether the use of "gateway" means that data must flow from a network to the firewall-IDS combination described by the patent, then to another network.

Each of the claims at issue (indeed, every independent claim in the '976 patent) recites in its preamble that it is a method or system for "detecting attacks *on a network*." The recipient of the attacks is the network (since a network is made up of the network devices it connects, an attack may be initiated by an attack [a transfer of data] addressed to a single network device, such as a particular CPU). Each claim then describes a "gateway" or "firewall" FN6 that is "receiving data from a remote source." That data is the potential medium of attack on the network. Unless the recipient allowed a single computer remote source to dial directly in on a dedicated private line, that remote source must be part of a network.

FN6. A firewall is a form of gateway. *See* Tr. at p. 87, ll. 9-11.

The specification sheds further light on the claim meaning by stating that "[t]he problem that we are addressing exists in the functioning of the Internet or any communications *network*. Such networks are inherently vulnerable to at least two types of attacks which disrupt or disable the functioning of *network services*." '976 patent, col. 1, ll. 6-10 (emphasis added).

Deep Nines argues that the specification of the '976 patent explicitly describes two gateways. One is the "gateway router **13"** of Fig. 1, which translates the addresses of data coming from Internet Service Provider **12** ("ISP") so the data is properly directed to its intended location. '976 patent, col. 3, ll. 15-25. The other gateway is the "customer gateway **14"** of Fig. 1. However, as seen in Fig. 1, these gateways, or this gateway system, receive data from the Internet **11** through the ISP **12;** in other words, the gateways receive data from a network. Any data that is not blocked by the patented firewall-IDS combination flows to the "public network" **101.** There is a network on each side of the gateways.FN7

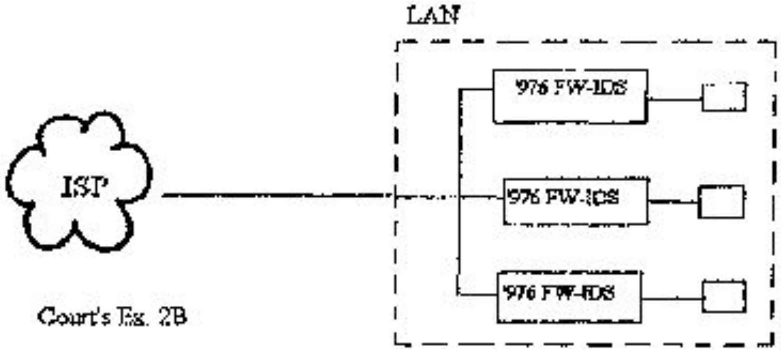
FN7. Customer gateway **14,** for example, connects two networks that use different technologies: the network bandwidth on the connection between gateway router **13** and customer gateway **14** is 1.544 Mbit, and the bandwidth on the connection between customer gateway **14** and the firewall/proxy **15** is 10 Mbit. *See* '976 patent, Fig. 1.

In support of its construction, Deep Nines references prior art cited in the prosecution history of the '976 patent. U.S. Patent 6,513,122 to Magdych ("the '122 patent") describes an "application gateway," which monitors ports receiving incoming connection requests and opens a connection for a particular port when it receives a request on that port. '122 patent, col. 2, ll. 11-27; *see also* Pl. Opening Br. at p. 22, [Doc. # 76]. U.S. Patent No. 6,182,226 to Reid ("the '226 patent") describes "application-level gateways" that are part of a firewall between networks and which transfer application data in a sanitized form between opposite sides of the gateway to prevent "a direct connection between the two different networks." '226 patent, col. 3, l. 66-col. 4, l. 10.

Just as in the '976 patent, these prior art references describe a gateway as something that translates or routes data from one network to another network. This comports with definitions found in technical dictionaries. "Gateway" is defined as: (1) A means by which users of one computer service or network can access certain types of information on a different service or network or (2) In networks, a device that connects two dissimilar local area networks ("LAN") or connects a local area network to wide-area network ("WAN"), a minicomputer, or a mainframe. *Webster's New World Dictionary of Computer Terms* 234 (7th ed.1999). The court will define this term as follows:

"Gateway" means "a device that connects two or more technologically different networks, enabling them to communicate."

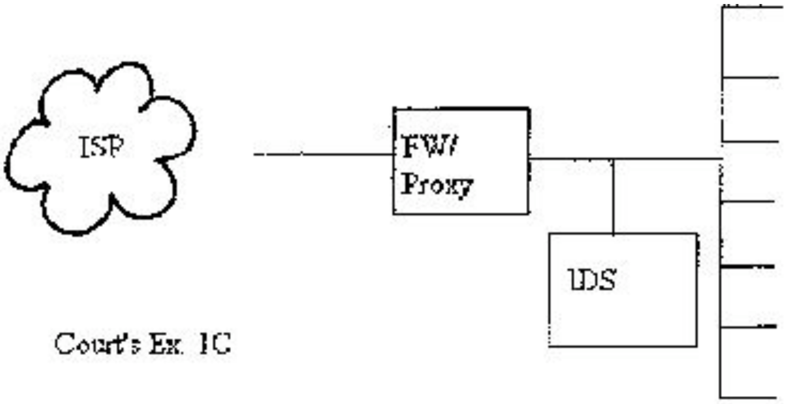
With this definition, the court does not intend to limit the scope of the claims only to systems with one gateway or only one application of the patented firewall-IDS combination. The parties agreed that Court's Ex. 2A diagrams a way in which a single application of the patented firewall-IDS combination would be a gateway between the ISP and a network. Tr. at p. 112, l. 20-p. 113, l. 12.



Court's Ex. 2B

This is similar to what is shown in Court's Ex. 1B. It also seems clear that a separate appliance programmed with the patented firewall-IDS gateway could be used to protect each host in a LAN. This was shown earlier in Court's Ex. 2B. *See* Tr. at p. 113, ll. 13-p. 115, l. 5. Although protection would not be as complete, a single host, or only some of the hosts, of a network could be protected by such separate appliances. *See*

Court's Ex. 3 (not discussed in transcript).



Court's Ex. 1C

If the attack is directed to a protected host, the patented firewall-IDS combination could provide protection. On the other hand, if the attack was directed to several or all of the hosts at once, including unprotected hosts that were turned on and connected to the network, then the attack might succeed.

4. "Target." '976 patent**, claims 6, 12, and 13.**

These claims describe receiving at a gateway or a gateway system "data from a remote source which is destined for a **target...."** Deep Nines proposes "a process on a computing device for which the data is destined." McAfee suggests "a network or a terminating device on the network." The parties' main point of contention is whether the target is a process (software) which will receive data, or whether it is a network or terminating device FN8 to which the attack is directed.

FN8. McAfee agreed at the hearing that "computer" would be an acceptable substitute for "terminating device." Tr. at p. 134, ll. 1-5.

The parties both cite to the '976 patent, col. 3, ll. 18-25, to support their respective interpretations. Deep Nines argues that this passage means that incoming data has an address location which is translated by a router, like gateway router **13.** Any requests directed to that address would be routed to the processor **101-1,** located in data storage **101.** What Deep Nines' quotation of this passage omits, however, is that the processors located in data storage **101** are *devices*. The specification of the '976 patent reinforces the point that the data from the remote source is destined for a device, rather than a process, in other places as well. *See, e.g.,* '976 patent, col. 5, ll. 44-46 (incoming data packets contain requests from the processors in data storage **101**); '976 patent, col. 4, l. 64-col. 5, l. 2 (incoming data packets are passed to the servers in data storage **101,** which handle the requests). Processors and servers are devices, not processes or software.

The prosecution history also supports the construction of "target" as a device rather than a process. The claims submitted to the Board of Patent Appeals and Interferences ("BPAI") demonstrate that the applicant considered the "target" to be the data storage **101** and private network **103** shown in Figure 1. BPAI Annotated Claims of 12/16/04, Def. Cl. Const. Br., Ex. 10 at p. 2 [Doc. # 80]; *see also* Third Preliminary Amendment of 9/23/03, Def. Cl. Const. Br., Ex. 4 at pp. 18, 20 ("target" in the claims is supported by element **103**); Second Preliminary Amendment of 4/30/03, Def. Cl. Const. Br., Ex. 6 at p. 15 (same).

One skilled in the art would also know that communication of information or data over a network can be conceptualized as occurring in layers, each with a header and some with address information. *See, e.g.,* Pl. Op. Br. at pp. 2-4 [Doc. # 76]; Def's *Markman* Presentation, Slide 26; *Computer Science and Communications Dictionary* 26 (2000) ("address" is an "a character or group of characters that identifies a data source or a data destination" or "refer[s] to a device or a data item by means of an identifying label.") A "target" is identified by the network-layer address: for example, the "www.anything" identified by the patentee. '976 patent, col. 3, ll. 20-25 These targets are identified in the '976 patent as "devices," col. 3, ll. 20-22, rather than applications.

A "target" is identified by a network-layer address, for example www.anything, which is translated by the detection/notification server 21(DNS). *See, e.g.,* '976 patent, col. 3, ll. 18-25, 56-60. The network-layer address in turn identifies the destination device, rather than the application. McAfee's construction of "target" is consistent with the way the '976 patent identifies the target with a network-level address, not an application. *See* col. 3, ll. 18-25; Figure 1 (data storage **101**).FN9

FN9. The application is identified by an additional layer of addressing: i.e., the port number in the transport layer, which the operating system uses to dispatch the data to the appropriate application. *See discussion in* Tr. at p. 119, l.11-p. 121, l. 13, p. 129, l. 3-p. 130, l. 22.

A court should avoid importing limitations from the specification into the claim terms, absent a clear disclaimer of claim scope. Phillips v. AWH Corp., 415 F.3d 1303, 1323 (Fed.Cir.2005) (*en banc*), *cert. denied,* 546 U.S. 1170, 126 S.Ct. 1332, 164 L.Ed.2d 49 (2006); Gillette Co. v. Energizer Holdings, Inc., 405 F.3d 1367, 1375 (Fed.Cir.2005). However, where, as here, the specification uses language of requirement, rather than preference, the specification describes an essential step or element of the claim, rather than merely a preferred embodiment. *See* Andersen Corp. v. Fiber Composites, Inc., 474 F.3d 1361, 1372-73 (Fed.Cir.2007), Honeywell Int'l v. ITT Indus., Inc., 452 F.3d 1312, 1318 (Fed.Cir.2006).

In this case, the specification of the '976 patent, the prosecution history, and the arguments the applicant made to the BPAI consistently associate "target" with a device. There is no hint anywhere in the patent itself or in the file history that the applicant intended "target" to also encompass processes or software. The court will therefore construe this term as follows:

"Target" means "the device or network identified by the network address for which the data is destined."

5. "Disconnecting the remote source." '976 patent**, claims 6, 12, and 13.**

An example of the use of the term is seen in claim 12 of the '976 patent, stating in part, with the disputed term in bold:

A method for detecting attacks on a network, comprising:....

acting on the data representing text identified as hostile in order to prevent an attack, wherein the data representing text identified as hostile is acted upon differently based on the type of the attack by at least one of blocking the data, alerting an administrator, and **disconnecting the remote source.**

Deep Nines initially suggested that the term be construed as "terminating the connection between the remote source and the target (i.e., blocking all data from the remote source)." McAfee proposed what it terms "ordinary meaning": "terminating the connection to the remote source." The parties agree that "disconnecting" in this context means "terminating," and that the connection to the remote source is what is terminated.

At the hearing, the parties agreed that "disconnecting the remote source" means "terminating the connection between the remote source and the target." Tr. at p. 137, ll.7-12. This is supported by the specification, and is in keeping with the ordinary meaning of the words. The parties also agreed that the IDS would perform the disconnecting. Tr. at p. 144, ll. 5-13. The remaining disagreement centered on the meaning of "target," which the court has already defined. Tr. at p. 138, l. 23-p. 143, l. 15. Accordingly the court defines this term as follows:

"Disconnecting the remote source" means "the IDS terminates the connection between the remote source and the target."

6. "Blocking the data." '976 patent**, claims 6, 12, and 13.**

An example of the use of the term is seen in claim 12 of the '976 patent, stating in part, with the disputed term in bold:

A method for detecting attacks on a network, comprising:....

acting on the data representing text identified as hostile in order to prevent an attack, wherein the data representing text identified as hostile is acted upon differently based on the type of the attack by at least one of **blocking the data,** alerting an administrator, and disconnecting the remote source ...

Deep Nines suggests that the term be construed as "stopping the data representing text identified as hostile from reaching the target." McAfee proposes "stopping the data representing text identified as hostile from reaching the [protected] network."

As with "intercepting in real time the remaining data," the dispute between the parties is at what location the data must be stopped. McAfee again argues that the applicant disclaimed the interception of data after it reaches the network in order to distinguish her invention over the Shipley reference during prosecution, while Deep Nines' proposal would theoretically allow the data to be blocked after it reaches the network, so long as it is stopped before it reaches the target.

The parties agreed that the words leading into the disputed phrase in the claims, "acting on the data representing text identified as hostile in order to prevent an attack," mean "taking an action that prevents an attack based on the data representing text identified as hostile." *See* Joint Claim Construction and Pre-Hearing Statement [Doc. # 65]. As discussed *supra,* the claims specify a gateway or a gateway system that receives data from a remote source. As the court has already stated, a gateway or gateway system enables data to flow from one network to another. The firewall-IDS combination is associated with the gateway or gateway system. The data not discarded by the firewall is detected and acted upon by the IDS before the data is sent to any network device. Therefore, the court construes this term as follows:

"Blocking the data" means "the IDS prevents the data representing text identified as hostile from reaching any network device."

7. "Remote source." '976 patent**, claims 6, 12, and 13.**

An example of the use of the term is seen in claim 12 of the '976 patent, stating in part, with the disputed term in bold:

A method for detecting attacks on a network, comprising: ... acting on the data representing text identified as hostile in order to prevent an attack, wherein the data representing text identified as hostile is acted upon differently based on the type of the attack by at least one of blocking the data, alerting an administrator, and disconnecting the **remote source.**

Deep Nines proposes "a process on a computing device that sends data to the target." McAfee suggests "a network or a terminating device on the network that sends data to the target." The basic dispute between the parties is similar to their disagreement over "target": i.e., whether or not the remote source sending data to the target is a network or device (McAfee) or a process on a computing device (Deep Nines).

At least the debate over "target" at the receiving end had something to do with the patented firewall-IDS combination. The term "receiving data from a remote source" is simply referring to the source of the attacks. The patentee was not trying to invent attack mechanisms or methods. The flow of the "data representing text identified as hostile" is from a network or "terminating device" to the patented firewall-IDS combination associated with a gateway. While the patentee gave examples of where the data came from, nothing in the ' 976 patent claims, specification, or prosecution history indicates that it matters whether the attacking data comes from one or more computers, other network devices or programs, or from the "network" itself. The court will construe this term as follows:

"Remote source" means "the network or device that sends the data received at the gateway that is associated with firewall and IDS."

8. "Active response module." "2 patent**, claim 1.**

"Selecting an active response module (ARM) from a plurality of available ARMs." "2 patent**, claim 1.**

"Linking said ARM to a computer misuse." "2 patent**, claim 1.**

An example of the use of these terms is seen in claim 1 of the "2 patent, stating in part, with the disputed terms in bold:

A method for automatically responding to an instance of computer misuse, comprising the steps of:....

(1) **selecting an active response module (ARM) from a plurality of available ARMs;**

(2) **linking said ARM to a computer misuse ...**

A. "Active Response Module (ARM)"

For this term, Deep Nines proposes "computer executable code defined by a common architecture that includes an arguments component, an action component, and an application program interface component." McAfee suggests "a module for providing an action in response to a computer misuse."

Deep Nines argues that the specification defines the architecture of the ARM as requiring an argument component, an actions component, and an application program interface. "2 patent, col. 5, ll. 40-42. McAfee counters that this is a preferred embodiment, and that the specification expressly envisions other types of architectures. *See, e.g.,* "2 patent, col. 5, ll. 42-46 ("It should be understood that other architectures for ARMs may be employed. Such other architectures will be apparent to one skilled in the relevant art(s) based on the discussion contained herein."). A court should not import limitations from the specification into the claim terms unless it is clear that the patentee intended them to be co-extensive. *See* Phillips v. AWH Corp., 415 F.3d 1303, 1323 (Fed.Cir.2005) (*en banc*), *cert, denied,* 546 U.S. 1170, 126 S.Ct. 1332, 164 L.Ed.2d 49 (2006).

In this case, the specification does not use "language of requirement," and the architecture described is just a preferred embodiment. The specification explicitly contemplates that the ARMs could have other architectures. Deep Nines argued at the hearing that the "fairly boilerplate statement" in the "2 patent that other architectures "will be apparent to one skilled in the relevant art(s)" should be discounted because these unidentified architectures are not disclosed in the patent. Tr. at p. 153, l. 25-p. 154, l. 11. Whether or not additional architectures are enabled or sufficiently disclosed by the specification, the "2 patent specifically envisions that such additional architectures exist and are covered by the patent.FN10 A construction which incorporates only this preferred embodiment is too narrow.

FN10. McAfee suggested at the hearing that another potential architecture for the ARM might be the "hardware" disclosed elsewhere in the "2 patent. Tr. at p. 165, ll. 1-5.

Deep Nines agreed at the hearing that a "module" in this context means a "program." Tr. at p. 156, ll. 3-7. The "2 patent specification states that the invention could be implemented using "hardware, software or a combination thereof." "2 patent, col. 15, ll. 24-25. The specification also explains that ARMs "process instances of computer misuse," and have the "means for instructing the data processing element to perform an action or series of actions in response to being involved by the misuse engine ." Col. 2, ll. 41-42, 52-54. The court will therefore construe this term as follows:

"Active response module" or "ARM" means "hardware, software, or a combination thereof that performs an action in response to a computer misuse."

B. "Selecting an active response module (ARM) from a plurality of available ARMs" and "linking said ARM to a computer misuse"

With respect to the first term, Deep Nines suggests "a user selecting an active response module (ARM) from a plurality of available ARMs." McAfee states that no further construction is required. For the second, Deep Nines proposes "a user associating the ARM to a computer misuse," while McAfee suggests "associating the ARM to a computer misuse." The basic dispute between the parties for both of these terms is whether the terms should be construed to require a user to perform the action in question.

Deep Nines argues that dependent claim 2, which recites "[t]he method of claim 1, wherein steps (l) [selecting]-(2) [linking] are performed using a graphical user interface," requires that a user perform steps (1) and (2) in claim 1. Deep Nines also points to the specification which, in a preferred embodiment, states that the user can perform these steps during the update process. *See* ' 942 patent, Abstract; col. 12, ll. 16-17, 30-35. McAfee counters that the specification demonstrates that the patentees were clearly aware of the term "user," but deliberately chose not to use the word in claim 1. McAfee also argues that claim 1 is not limited to the update process embodiment Deep Nines points to.

Deep Nines agreed at the hearing that the process of selecting the ARM *could* be automated, but insisted that the "2 patent only discloses the system where the human user or system administrator performs the selection. Tr. at p. 157, ll. 5-14. However, Figure 6 of the "2 patent specifically envisions an embodiment where the IDS identifies the ARM, meaning that no user involvement would be necessary. In addition, the preamble to claim 1 states that the claim recites a series of steps for practicing the method of *automatically* responding to an instance of computer misuse. "2 patent, col. 16, ll. 56-57 (emphasis added). In light of these disclosures, interpreting the claim language to require that a user perform the selection and linking steps would improperly import a limitation from the specification into the claims.

At the hearing, McAfee expressed concern over an additional phrase in claim 1 of the "2 patent, "receiving by said ARM, data pertinent to said instance of said computer misuse," arguing chiefly that Deep Nines' position that the data had to be received from an IDS was incorrect. The parties had previously agreed that this term required no construction. However, McAfee spent some time at the hearing arguing that the data could also be received from "other devices," although it was only able to suggest a firewall as an alternative. Tr. at p. 169, l. 3-p. 170, l. 14.

The "2 patent repeatedly states that the ARM receives data from the IDS. *See, e.g.,* Abstract ("Upon receipt of an instance of the computer misuse from the intrusion detection system, each ARM linked to the misuse collects pertinent data from the intrusion detection system ...); Summary of Invention, "2 patent, col. 2, ll. 40-44 ("The method for automatically responding to a computer miscue includes the steps of defining a plurality of ARMs to process instances of computer misuse, receiving an instance of misuse from an intrusion detection system ..."); "2 patent, col. 2, l. 65-col. 3, l. 1 ("New ARMs may be defined and deployed in a 'plug and play' manner into an existing computing environment that utilizes any type of intrusion detection system."). These references all occur in the "Abstract" or "Summary of Invention" sections, which do not describe preferred embodiments.

McAfee points to col. 4, ll. 41-48 of the "2 patent ("after reading the following description, it will be apparent to one skilled in the relevant art(s) how to implement the following invention in alternative embodiments"). Even this example of an alternative embodiment states that the ARM receives data from the IDS. *See* "2 patent, col. 4, ll. 45-58.

Both sides agree that "linking" should be construed as "associating." The court will therefore construe these terms as follows:

"Selecting an active response module (ARM) from a plurality of available ARMs" requires no construction beyond the court's previous definition of "active response module."

"Linking said ARM to a computer misuse" means "associating the ARM to a computer misuse."

"Receiving by said ARM, data pertinent to said instance of said computer misuse" means "the ARM receiving data from an intrusion detection system for the instance of the computer misuse."

9. "Client computers with firewalls." '292 patent**, claims 1 and 8.**

An example of the use of this term is seen in claim 1 of the '292 patent, stating in part, with the disputed term in bold:

A method for monitoring intrusion activity utilizing a plurality of firewalls, comprising:..

(a) establishing network communications between a server computer and a plurality of **client computers with firewalls....**

Deep Nines proposes "each equipped with a firewall." McAfee suggests no construction is necessary. Should the court decide to construe the term, McAfee proposes "interfaced to firewalls." The parties agree on the definitions of "client computers" and "firewall"; the only dispute remaining is whether the court should construe "with" and, if so, how.

Deep Nines argues that the court should construe "with" to mean "each equipped with." In support of this position, it points to the language in claims 1 and 8 that once the information has been collected from the firewalls of the client computers, a response is transmitted "to the firewalls of *each* of the plurality of client computers utilizing the network." '292 patent, col. 7, ll. 18-19 (emphasis added); *see also* '292 patent, col. 3, ll. 16-17 ("A plurality of data computers **104** or user computers **106** may be each equipped with a firewall."). Deep Nines also points to an amendment made during prosecution of the '292 patent, in which the applicant changed "transmitting a response to the firewalls of the computers utilizing the network" to the present language, "transmitting a response to the firewalls of each of the plurality of client computers utilizing the network," in order to overcome a prior art reference. Amendment of 12/12/05, Pl. Resp. Cl. Const. Br., Ex. B1 at 2 [Doc. # 79]. Clearly, Deep Nines argues, this is evidence that "with" is intended to mean "each equipped with." McAfee counters that there is an alternate, viable meaning of "with" that this construction excludes, namely that each plurality of computers may share a plurality of firewalls in something other than a one-to-one relationship.

During prosecution, the applicants amended their claims in order to distinguish their invention over U.S. Patent No. 5,991,881 ("the Conklin reference").FN11 In doing so, the applicants noted that Conklin showed one IDS in communication with the operating system of one computer, rather than the "plurality of computers with firewalls," the applicants claimed. A prosecution disclaimer must be "both clear and unmistakable to one of ordinary skill in the art ." *Elbex* Video, Ltd. v. Sensormatic Elec. Corp., 508 F.3d 1366, 1371-72 (Fed.Cir.2007) (citing cases in which no clear disclaimer was present).

FN11. The Conklin patent is incorrectly cited as U.S. Patent No. 5,796,942 in the Amendment of 12/12/05, Pl. Resp. Cl. Const. Br., Ex. B1 at 9 [Doc. # 79].

Here, the prosecution disclaimer was as unmistakable as *Elbex Video* requires. Conklin disclosed a one IDS/one computer system, and it is not clear whether the applicants distinguished Conklin on the basis of the number of computers, the number of firewalls, or that the present invention claimed a plurality of computers, each with its own firewall (as Deep Nines argues). When the applicants amended their claims, they chose to have the word "each" modify the "plurality of client computers," rather than each computer individually. Further, the applicants stated only that Conklin failed to teach "client computers with firewalls," not "client computers, *each* with a firewall," as Deep Nines contends. Amendment of 12/12/05, Pl. Resp. Cl. Const. Br., Ex. B1 at 10 [Doc. # 79].

Therefore, in light of the specification, which discloses Deep Nines' proposed construction only in a preferred embodiment, and the prosecution history, which does not contain a clear disclaimer by the applicants, the court will construe this term as follows:

"Client computers with firewalls" means "two or more client computers are protected by two or more firewalls that each may protect one or more of the computers."

10. "Predetermined profiles." '128 patent**, claims 12 and 23. "Predetermined indicators."** '128 patent**, claims 12 and 23.**

An example of the use of these terms is seen in claim 23 of the '128 patent, stating in part, with the disputed terms in bold:

A method for assessing threats to a network utilizing a plurality of data sources, comprising ...

Performing threat assessment profiling by generating an alert upon successfully comparing **predetermined profiles** with the aggregated and correlated network data ...

Performing threat assessment predicting by:

generating an alert upon successfully comparing the **predetermined indicators** with the aggregated and correlated network data ...

Deep Nines proposes "profiles [indicators] determined before collecting network data from the plurality of diverse network data sources." McAfee suggests "a profile [indicator] determined no later than at the time of performing threat assessment profiling [predicting]." The parties' conflict over these terms is one of timing: Deep Nines argues that the profiles and indicators must be determined before the network data is collected. McAfee counters that they should be determined at the point when the threat assessment profiling or prediction is taking place.

To support its argument, Deep Nines cites col. 9, l. 64-col. 10, l. 1 of the ' 128 patent, which describes a scenario in which the predetermined indicators are determined before the network data is collected, and col. 9, ll. 24-31, describing a cycle where the predetermined profile is determined before the network data is mined. McAfee argues that Deep Nines' construction would exclude a preferred embodiment, and points to col. 10, ll. 4-12 of the '128 patent ("During the course of such [data] mining, predetermined indicators are compared with the aggregated and correlated network data and the results of the method **400** of Fig. 4.").

A claim construction that excludes a preferred embodiment is rarely, if ever, correct. Sandisk Corp. v. Memorex Prods., Inc., 415 F.3d 1278, 1285 (Fed.Cir.2005). Deep Nines argues strenuously that "predetermined" must mean that the profile is generated before the network data is mined, but in the scenario described in col. 10, ll. 4-12, the profile is clearly generated after collecting the network data. This passage, as well as Figure 6, describes the case in which the profiles are updated during the mining process. Because the mining process cannot begin until the network data has been collected, some predetermined profiles must therefore be created after the network data has been collected. "Predetermined" in this context refers to the threat assessment profiling, which occurs after the profile is generated. Adopting Deep Nines' construction would exclude this embodiment.

The claim language supports such an interpretation as well. Claim 12 recites "computer code for performing threat assessment profiling by generating an alert upon successfully comparing predetermined profiles with the aggregated and correlated network data ..." Col. 12, ll. 13-16. The claim goes on to state that threat assessment predicting is done by generating a profile "upon successfully comparing" the predetermined indicators with the aggregated and correlated network data. Col. 12, ll. 24-27. There is nothing in this language that limits "predetermined" to the time before the network data is collected; to the contrary, the claim language indicates that the profile and indicators are generated after the data has been collected. The only limitations are those suggested by McAfee: that the profile be generated before the threat assessment profiling is done, and the indicators be determined before threat assessment predicting is performed.

With respect to predetermined indicators, there is also nothing in the specification or claims that limits "predetermined" to the time before the network data is collected. Doing so would exclude a scenario where the predetermined indicators are determined while network data is collected. Specifically, the specification states that the predetermined indicators may include portions of the predetermined profiles. '128 patent, col. 9, ll. 58-62. Because the predetermined profiles can be determined after the network data collection begins, the indicators may contain portions of those profiles. *See, e.g.,* '128 patent, col. 10, ll. 4-10. Requiring the indicators to be determined prior to the collection of network data would contravene this clear language in the specification. The court will therefore construe these terms as follows:

"Predetermined profiles" means "profiles determined no later than at the time of performing threat assessment profiling."

"Predetermined indicators" means "indicators determined no later than at the time of performing threat assessment predicting ."

11. "... results of monitoring the network data." '128 patent**, claim 12. "... the results."** '128 patent**, claim 12.**

An example of the use of these terms is seen in claim 12 of the '128 patent, stating in part, with the disputed terms in bold:

A computer program product for assessing threats to a network utilizing a plurality of data sources, comprising ...

computer code for **performing threat assessment profiling by generating an alert upon successfully comparing predetermined profiles with the aggregated and correlated network data and results of monitoring the network data;** and

computer code for performing threat assessment predicting by

generating an alert upon successfully comparing the predetermined indicators with the aggregated and correlated network data and the results, and generating a profile upon successfully comparing the predetermined indicators with the aggregated and correlated network data and **the results....**

Deep Nines suggests that both terms are indefinite for lack of antecedent basis. McAfee argues that neither term is indefinite.

The oft-cited maxim that "claim language should generally be construed to preserve validity, *if possible,*" Tate Access Floor Inc. v. Interface Arch. Res. Inc., 279 F.3d 1357, 1367 (Fed.Cir.2002) (emphasis in original), applies only in the case where the court concludes, after applying all the available canons of claim construction, that the term at issue is still ambiguous. *See* Liebel-Flarsheim Co. v. Medrad, Inc., 358 F.3d 898, 911 (Fed.Cir.2004).

In that situation, claims can be construed to preserve their validity "where the proposed claim construction is 'practicable,' is based on sound claim construction principles, and does not revise or ignore the explicit language of the claims." Generation II Orthotics, Inc. v. Medical Tech. Inc., 263 F.3d 1356, 1365 (Fed.Cir.2001). As a general rule, however, claims

need not be plain on their face in order to avoid condemnation for indefiniteness; rather, what [the court will ask] is that the claims be amenable to construction, however difficult that task may be ....[t]he test for indefiniteness does not depend on a potential infringer's ability to ascertain the nature of its own accused product to determine infringement, but instead on whether the claim delineates to a skilled artisan the bounds of the invention.

Smith Kline Beecham Corp. v. Apotex Corp., 403 F.3d 1331, 1340-41 (Fed.Cir.2005).

"The requirement of antecedent basis is a rule of patent drafting, administered during patent examination." Energizer Holdings, Inc. v. Int'l Trade Comm'n, 435 F.3d 1366, 1370 (Fed.Cir.2006). However, "the failure to provide explicit antecedent basis for terms does not always render a term indefinite." *Id.* (quoting the Manual of Patent Examining Procedure, s. 2173.05(e)). Whether a claim lacking a specific antecedent basis "nonetheless has a reasonably ascertainable meaning must be decided in context." *Id.*

Deep Nines argues that both terms are indefinite because they lack an antecedent basis; in other words, because there is no step in claim 12 that specifies what the results of the monitoring are, the claims are indefinite. McAfee suggested at the hearing that a person of skill in the art would understand these terms to mean monitoring any number of things, including the bandwidth, the destination distribution of addresses, the type of protocols, or the particular content of data packets. Tr. at p. 219, ll. 2-7. It points to the '128 patent, col. 7, ll. 56-62, which states that the network data may be monitored using a baseline monitoring application that produces, for example, enhanced threshold-based alerts. The specification further explains that this can be accomplished by network adaptive baseline monitoring module **210** (Figure 2), and that more information regarding monitoring can be found in Figure 4.

While the claim language in question is broad, McAfee has pointed to a portion of the specification that describes one way the "monitoring" can be performed. In light of this disclosure, the court declines to find that the terms are indefinite, as Deep Nines urges.

IV. CONCLUSION

The jury shall be instructed in accordance with the court's interpretation of the disputed claim terms in the '976, "2, 252, and '128 patents.

So **ORDERED.**

E.D.Tex.,2008.
Deep Nines, Inc. v. McAfee, Inc.

Produced by Sans Paper, LLC.