IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

FORTINET, INC., Plaintiff, v. SRI INTERNATIONAL, INC., Defendant. _______________________/	No. C 12-02540 JSW **TENTATIVE RULINGS AND QUESTIONS RE CLAIM CONSTRUCTION**
CHECK POINT SOFTWARE TECHNOLOGIES, INC., Plaintiff, v. SRI INTERNATIONAL, INC., Defendant. _______________________/	No. C 12-03231 JSW

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD, PLEASE TAKE NOTICE OF THE FOLLOWING TENTATIVE RULING AND QUESTIONS FOR THE HEARING SCHEDULED ON OCTOBER 8, 2013, AT 1:30 p.m.:

The Court has reviewed the parties' briefs and, thus, does not wish to hear the parties reargue matters addressed in those pleadings. If the parties intend to rely on legal authorities not cited in their briefs, they are ORDERED to notify the Court and opposing counsel of those authorities reasonably in advance of the hearing and to make copies available at the hearing. If the parties submit such additional authorities, they are ORDERED to submit the citations to the authorities only, without argument or additional briefing. *Cf.* N.D. Civil Local Rule 7-3(d). The parties will be given the opportunity at oral argument to explain their reliance on such authority. The Court suggests that associates or of counsel attorneys who are working on this case be permitted to address some or all of the Court's questions contained herein.

The parties shall each have 60 minutes to present their respective arguments on claim construction. The Court provides its tentative constructions of the disputed terms.

1. "Network monitors"/"the monitors"

The term "network monitors appears in Claims 1, 4, 6, 13, 16, and 18 of the '615 Patent, and Claims 1, 4, 6, 12, 15, and 17 of the '203 Patent. The term "the monitors" appears in Claim 1 of both the '615 and the '203 Patents. The parties agree that "the monitors" refers to "network monitors."

SRI argues that the term "network monitors" must be construed to mean "software and/or hardware that can collect, analyze and/or respond to data." (Parties' Final Joint Claim Construction Statement ("Statement") at App. A.) Fortinet and Check Point (collectively, "the Plaintiffs"), on the other hand, argue that the term must be construed to mean "software and/or hardware that can detect suspicious activity by analyzing network traffic data." (*Id.*)

It appears that the key dispute between the parties is whether all "network monitors" must be capable of detecting suspicious activity through the analysis of network traffic data. SRI argues that the construction the Plaintiffs advance would improperly require hierarchical monitors to include this capability. SRI further contends that the Plaintiffs' proposed construction creates a redundancy in the claim language. What is the Plaintiffs' best argument that it is not confusing and redundant to construe "network monitors," in the context of the claim, to read "detecting, by the 'software and/or hardware that can detect suspicious activity by analyzing network traffic data,' suspicious network activity based on analysis of network traffic data"?

The Court **tentatively** adopts the following construction: "software and/or hardware that can collect, analyze and/or respond to data."

2. "Suspicious network activity"

The term "suspicious network activity" appears in Claims 1 and 13 of the '615 Patent, and Claims 1 and 12 of the '203 Patent.

SRI argues that the term "suspicious network activity" must be construed to mean "activity that indicates a known or possible malicious attack on the network." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "network traffic with attributes of a suspected, but unconfirmed, intrusion." (*Id.*)

The key areas of dispute between the parties are: (1) whether "suspicious network activity" can encompass known attacks; and (2) whether "network activity" is synonymous with "network traffic." How does SRI contend that "suspicious network activity" can include known threats, when the Patent specifications distinguish between "intrusion reports" relating to known malicious activity, and "suspicion reports" that presumably relate to unconfirmed threats? (*See* '203 Patent at 7:38-45.) Additionally, why does SRI argue that it is improper to construe "network activity" as "network traffic" when the Patent specifications appear to use the terms interchangeably? (*Compare* '203 Patent at 11:41-44 *with id.* at 1:55-57.)

The Court **tentatively** adopts the following construction: "network traffic with attributes of a suspected, but unconfirmed, intrusion."

3. "Automatically receiving and integrating"

The term "automatically receiving and integrating" appears in Claim 1 of both the '615 and the '203 Patents.

SRI argues that the term "automatically receiving and integrating" must be construed to mean "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product; i.e., something more than simply collecting and reiterating data." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product (i.e., something more than simply collecting and reiterating data) for purposes of detecting a suspected attack or threat." (*Id.*)

The key dispute between the parties is whether detecting a suspected attack or threat is the sole purpose of "automatically receiving and integrating." How do the Plaintiffs reconcile this proposed limitation with language in the specifications that sets forth other goals for integration, such as alerting other network entities, identifying attacks to other network entities, and determining the proper response in which the system should engage? (*See* '203 Patent at 2:10-14, 3:23-42.)

The Court **tentatively** adopts the following construction: "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product; i.e., something more than simply collecting and reiterating data."

4. [hierarchical monitors] "adapted to automatically receive and integrate"

The term [hierarchical monitors] "adapted to automatically receive and integrate" appears in Claim 13 of the '615 Patent and Claim 12 of the '203 Patent.

SRI argues that the term [hierarchical monitors] "adapted to automatically receive and integrate" must be construed to mean "capable of receiving reports of suspicious activity and, without user intervention, combining those reports into a different end product; i.e., something more than simply collecting and reiterating data." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term "adapted to" does not be construed, and the remainder of the term must be construed to mean "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product (i.e., something more than simply collecting and reiterating data) for purposes of detecting a suspected attack or threat." (*Id.*)

The key dispute between the parties is whether "adapted to" should be construed as synonymous with "capable of." How does SRI respond to case law indicating that "adapted to" is most commonly defined more narrowly than "capable of"? *See, e.g., Aspex Eyewear, Inc. V. Marchon Eyewear, Inc.*, 672 F.3d 1335, 1349 (Fed. Cir. 2012); *Brocade Commc'ns Sys., Inc. V. A10 Networks, Inc.*, No. C 10-3428 PSG, 2013 WL 831528, at *10-11 (N.D. Cal. Jan. 10, 2013).

The Court **tentatively** adopts the following construction: "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product; i.e., something more than simply collecting and reiterating data."

5. "Detecting, by the network monitors, suspicious activity based on analysis of network traffic data"

The term "detecting, by the network monitors, suspicious activity based on analysis of network traffic data" appears in Claim 1 of both the '615 and '203 Patents.

SRI argues that the term "detecting, by the network monitors, suspicious activity based on analysis of network traffic data" must be construed to mean "detecting based on an analysis of data derived from or describing network packets and excluding analysis that is limited solely to host operating system audit logs." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "detecting, by the network monitors, suspicious network activity based on direct examination of network packets." (*Id.*)

The key dispute between the parties is whether "detecting" requires direct examination of data. Why is SRI not estopped from arguing for its proposed construction by its express assertions during reexamination that "analysis of network traffic data" requires direct examination of network packets? (*See, e.g.*, Appeal Brief at 7; Reply Brief at 5.)

The Court **tentatively** adopts the following construction: "detecting, by the network monitors, suspicious network activity based on direct examination of network packets."

6. "Said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data"

The term "said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data" appears in Claim 13 of the '615 Patent and Claim 12 of the '203 Patent.

SRI argues that the term "said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data" must be construed to mean "capable of detecting based on an analysis of data derived from or describing network packets and excluding analysis that is limited solely to host operating system audit logs." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "said plurality of network monitors detecting suspicious network activity based on direct examination of network packets." (*Id.*)

The key dispute between the parties – apart from that described above in Claim term 5 – is whether the network monitors must be actively detecting suspicious network activity, or merely capable of performing that function. How does SRI reconcile its proposed construction with the Claim language indicating that the network monitors are already deployed and actively detecting suspicious network activity? (*See* '203 Patent, Claim 12.)

The Court **tentatively** adopts the following construction: "said plurality of network monitors detecting suspicious network activity based on direct examination of network packets."

7. "Network monitors deployed"/"network monitors are deployed"

The terms "network monitors deployed"/"network monitors are deployed" appears in Claims 13 and 18 of the '615 Patent, and Claims 12 and 17 of the '203 Patent.

SRI argues that the terms "network monitors deployed"/"network monitors are deployed" must be construed to mean "network monitors that can be configured and/or installed." (Statement at App. A.) The Plaintiffs, on the other hand, note that the parties agree that "deploying a plurality of network monitors" means "configuring and/or installing two or more network monitors," and that "software is configured and hardware is installed." (*Id.*) The Plaintiffs contend that this claim term does not require additional construction, but argue that if the Court construes the term, it must be construed to mean "network monitors that are configured and/or installed" and that "software is configured and hardware is installed." (*Id.*)

The key dispute between the parties is whether "deployed" means that the network monitors are configured or installed, or merely capable of being configured or installed.

The Court **tentatively** adopts the following construction: "network monitors that are configured and/or installed" and "software is configured and hardware is installed."

8. "Correlating intrusion reports reflecting underlying commonalities"

The term "correlating intrusion reports reflecting underlying commonalities" appears in Claim 2 of both the '615 and the '203 Patents.

SRI argues that the term "correlating intrusion reports reflecting underlying commonalities" must be construed to mean "combining the reports to reflect underlying commonalities." (Statement at App. A.) Check Point agrees with SRI's proposed construction. (*Id.* at 2 n.1.) Fortinet, on the other hand, argues that the term either needs no construction, or in the alternative, it must be construed to mean "combining intrusion reports with underlying commonalities to identify more global threats." (*Id.* at App. A.)

The key dispute between SRI and Fortinet is whether the sole purpose of combining the reports is to identify more global threats to the network. What is Fortinet's best argument that the purpose of combining reports should be solely to identify more global threats?

The Court **tentatively** adopts the following construction: "combining the reports to reflect underlying commonalities."

9. "Correlating intrusion reports reflecting underlying commonalities"

The term "correlating intrusion reports reflecting underlying commonalities" appears in Claim 14 of the '615 Patent, and Claim 13 of the '203 Patent.

SRI argues that the term "correlating intrusion reports reflecting underlying commonalities" in the context of these Claims must be construed to mean "capable of combining the reports to reflect underlying commonalities." (Statement at App. A.) The Plaintiffs do not believe this term needs additional construction but argue that it must be construed consistently with Claim term 8, above. (*Id.*)

The key dispute between the parties is whether integration requires hierarchical monitors to be correlating reports or whether it merely requires that they possess the capability to correlate reports. How does SRI respond to the Plaintiffs' contention that the claimed system does not exist unless the hierarchical monitors are actually correlating reports?

The Court **tentatively** adopts the following construction: "combining the reports to reflect underlying commonalities."

10. "Network traffic data"

The term "network traffic data" appears in Claims 1 and 13 of the '615 Patent, and Claims 1 and 12 of the '203 Patent.

SRI does not believe that this term requires construction. (Statement at App. A.) However, should the Court construe the term, SRI argues that the term "network traffic data" must be construed to mean "data derived from or describing network packets." (*Id.*) The Plaintiffs, on the other hand, argue that the term must be construed to mean "network traffic data" is comprised of "network packets." (*Id.*)

The key dispute between the parties is whether network traffic data can be equated with network packets. What is SRI's best argument that it should not be bound by its own statement during reexamination that "the phrase 'network traffic data' refers to data obtained from network traffic, i.e., network packets"?

//

//

United States District Court
For the Northern District of California

The Court **tentatively** adopts the following construction: "network traffic data" is comprised of "network packets."

IT IS SO ORDERED.

Dated: October 3, 2013

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE