HIGHLY CONFIDENTIAL – SOURCE CODE
REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED
DECLARATION OF DR. MICHAEL MITZENMACHER

I, Michael Mitzenmacher, hereby declare that:

1. I have been asked by Plaintiff Finjan, Inc. to submit an expert declaration on whether Juniper, Inc.'s SRX Gateways, Sky ATP and ATP Appliance products infringe claim 1 of U.S. Patent No. 8,141,154 (the "'154 Patent"). Ex. 1.[1] I relied on the documents cited herein, including the '154 Patent, the file history of the '154 Patent, the source code, the deposition transcripts of Tenorio, Manthena, Nagarajan, and Manocha, the trial transcript for this case, exhibits thereto, Finjan's Infringement Contentions, and Juniper's Discovery Responses.

I. EXPERIENCE AND QUALIFICATIONS

2. I received a Ph.D degree in Computer Science from the University of California at Berkeley in 1996. I am currently employed as a Professor of Computer Science at Harvard University. I have published over 200 research papers in computer science conferences and journals, many of which have explored computer securities and computer networks, such as algorithms and data structures for communication networks and data transmission. I regularly serve on program committees for conferences in networking, algorithms, and communication, including SIGCOMM, NSDI, and CoNEXT. I have also taught graduate courses relating to computer networking.

3. My rate of compensation for my work in this case is $750 per hour plus any direct expenses incurred. My compensation is based solely on the amount of time that I devote to activity related to this case and is in no way affected by any opinions that I render. I receive no other compensation from work on this action. My compensation is not dependent on the outcome of this case.

II. LEGAL STANDARDS

4. Counsel for Finjan has informed me of the following legal standards that I have used as a framework in forming my opinions contained herein.

5. I have been informed that claim construction is a legal issue for the Court to decide. I also understand that the Court has not issued a claim construction order for the '154 Patent in this case. As such, I considered both parties' proposed constructions of disputed terms and applied the plain and ordinary meaning for all other terms.

[1]

6. I have been informed that infringement is determined on a claim by claim basis. A product may infringe a claim either literally or under the doctrine of equivalents.

7. I have been further informed that literal infringement is found if an accused product, system or method meets each and every element of a single claim. Direct infringement is found if a party, or its agents, makes, uses, sells, or offers for sale a product or system that contains all elements of a claimed system or performs all of the steps of a claimed method. I have been informed that a party can be found to use the patented system even if that party does not exercise physical or direct control over every element of the system. I have been informed that for elements that are not subject to the physical or direct control of the party, that party is still deemed to be using that component or part of the patented system where the party (i) puts the component into service – that is, the party causes it to work for its intended purpose and (ii) receives the benefit of that purpose. I have been informed that direct infringement can be found in a multinational system claim where elements of such system are located in multiple countries, when the place where control of the accused system is exercised and where beneficial use of the system is obtained are both within the United States.

8. I have been informed that infringement under the doctrine of equivalents is found if an accused product, system or process contains parts or steps that are identical or equivalent to each and every element of a single claim. A part or step is equivalent if a person of ordinary skill in the art ("POSITA") would conclude that, at the time of infringement, the differences between the product or method step and the claim element were not substantial. One common test to determine if the difference between a component or method step and a claim element is not substantial is to determine whether the component or step performs substantially the same function, in substantially the same way, to achieve substantially the same result.

9. Based on review of the Asserted Patents and consideration of the abovementioned factors, it is my opinion that a person of ordinary skill in the art at the time of the invention of the Asserted Patents would be someone with a bachelor's degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field. I understand that claim 1 of the '154 Patent claims a priority date of December 12, 2005. But if the '154 Patent is found to have another priority date it would not materially affect my

analysis.

III. SUMMARY OF DECLARATION

10. I have been asked by counsel for Finjan to consider if Juniper infringes claim 1 of the '154 Patent. I have assumed that claim 1 of the '154 Patent is valid and enforceable. I have not considered damages related issues associated with this infringement.

11. The language of claim 1 is set forth in the '154 Patent at 17:31-44.

12. I have been asked by counsel for Finjan to consider the following infringement scenarios with respect to claim 1 of the '154 Patent: (1) SRX Gateways ("SRX") by themselves, (2) SkyATP by itself, (3) ATP Appliance by itself. My opinion on the current product features is based on the information available, including source code, release notes, Juniper's documents, and deposition testimonies of Juniper's employees.

IV. OVERVIEW OF THE '154 PATENT

13. The '154 Patent describes protecting a computer system from dynamically generated malicious content. *See* '154 Patent, Abstract. Many types of documents (such as PDF, Office, HTML) allow for generating content dynamically. As one example, a document may be embedded with a JavaScript ("JS") script, which is able to call a link from which to download a file. As another example, an iFrame (which is another HTML document embedded into the main HTML page) inserts external content into the main HTML page, and thereby allows for dynamically generated malicious content. As a further example, an email or a document may include an HTTP link to a site. The HTTP link by default is associated with an HTTP function (such as an HTTP GET request), which allows a computer to automatically communicate with the site hosted by the HTTP link upon the activation of the HTTP link.

14. The ability to dynamically generate content allows malicious code to evade detection through obfuscation. Obfuscation is a mechanism which allows malicious code to be encoded or reformatted in a string that it appears to be benign, but the encoded or reformatted string is later decoded or reformatted to generate the malicious code for execution. *See* '154 Patent at 3:31-64 (describing how dynamically generated content would result in malicious code being inserted). Obfuscation is one way in which activation of a seemingly benign link may result in malicious code being injected into a

document or causing a malware to be downloaded. Dynamically generated malicious content typically comes in the form of a multi-stage attack such as a drive-by Download, or through a link on a webpage or email. Ex. 15, FINJAN-JN 045339 at 41 (describing the mechanism of a drive-by Download attack); FINJAN-JN 045326 at 29-30 (describing different ways ransomware infects a computing system). The dynamically generated malicious code cannot be detected by conventional reactive content inspection or gateway level analysis because the malicious code is not present in the content before runtime, which is when the malicious code is generated. '154 Patent at 3:65-4:8. Claim 1 of the '154 Patent describes the use of a content processor to process content which includes a call to a first function and the call has an input. *See id.*, Claim 1. The '154 Patent also recites sending the input to a security computer for inspection. *See id.* Claim 1 also recites invoking a second function with the input only if a security computer indicates that it is safe to invoke the second function. *Id.* By utilizing "behavioral analysis technologies," Claim 1 of the '154 Patent allows a security system to detect "day-zero" threats which escape the detections by traditional security technologies.

V. OVERVIEW OF THE ACCUSED PRODUCTS

A. SRX Gateways

15. SRX is the next generation security gateway that provides essential capabilities to protect a network of computers such as a corporate network. The SRX Gateways operate as a gateway between the untrusted Internet and a trusted internal network. Ex. 9, JNPR-FNJN_29002_00173278 at 84. It is my understanding that the SRX all operate using the Junos operating system. The SRX Gateways can receive content (such as network communications, downloaded files) from the Internet, can send objects such as files and URLs to Sky ATP or ATP appliance for analysis, can receive a result from Sky ATP or Appliance, and can take an action (such as blocking or allowing files or network communications) based on the result received from Sky ATP or ATP Appliance. *Id.*; *see also* Ex. 6, JNPR-FNJN_29018_00962784 at 91-92. This process allows the SRX to detect new viruses and zero-day threats before they harm the computers in the protected network.

B. Sky ATP

16. Juniper Sky ATP is a cloud-based scanning system that is part of Juniper's Advanced Anti-Malware Solution "AAMW". Ex. 9, JNPR-FNJN_29002_00173278 at 83. Sky ATP sometimes

is also referred to as Argon or Argon cloud. *Id.* Sky ATP can be used as a service by SRX Gateways. *Id.* (showing that AAMW solution integrates with SRX and Argon Cloud Server). SRX can submit files or URLs to Sky ATP for analysis and Sky ATP will return a verdict and threat intelligence data feeds including black/white lists. *Id.* at 83-84. The results are returned in the JSON format includes verdict information such as sample ID, malware info, malware among others,. *See, e.g.*, Ex. 2, JNPR-FNJN_29017_00553620 at 74 (describing fields for malware event data and host threat level/status change data).

17. In particular, Sky ATP provides advanced anti-malware and anti-ransom protection against sophisticated "zero-day" and unknown threats. *See* Ex. 13, FINJAN-JN 044887 at 905 (stating that Sky ATP protects against evolving security threats); Ex. 9, JNPR-FNJN_29002_00173278 at 83. Sky ATP generates "actionable intelligence" that can be used in a security network to take an action based on the threats discovered by Sky ATP. Ex. 9, JNPR-FNJN_29002_00173278 at 83-84. Sky ATP includes a malware pipeline manager; a file runs through the malware analysis pipeline, which includes adapters for performing a series of analyses, based on cached results, antivirus analysis, static analysis, and dynamic analysis. Ex. 13, FINJAN-JN 044887 at 907. The malware analysis includes an antivirus adapter, two static adapters, and a sandbox and deception adapters. Ex. 14, JNPR-FNJN_29017_00552908 at 909.

18. Sky ATP performs static analysis to determine if unusual operations are used and dynamic analysis to identify behaviors of the file. Ex. 13, FINJAN-JN 044912. Sky ATP has a static analysis component that is run on the input it receives. *See id.* The static analysis in Sky ATP inspects file's metadata and instruction categories to detect suspicious signs such as usual instructions. *Id.* Static analysis analyzes the metadata information, categories of instructions used, and file entropy (e.g., encryptions in a file), feeds the outputs into a machine learning algorithm to generate a verdict. *Id.* Sky ATP performs dynamic analysis by executing the content in a sandboxed environment as if the file is run in a real computer system. *Id.* As part of the "detonation" of the file, the sandbox environment records the operations performed by content. *Id.* It is my understanding that Juniper internally refers to the dynamic analysis performed in the malware inspection pipeline as the combination of the "deception adapter" and a sandbox called "Joe Sandbox."

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.