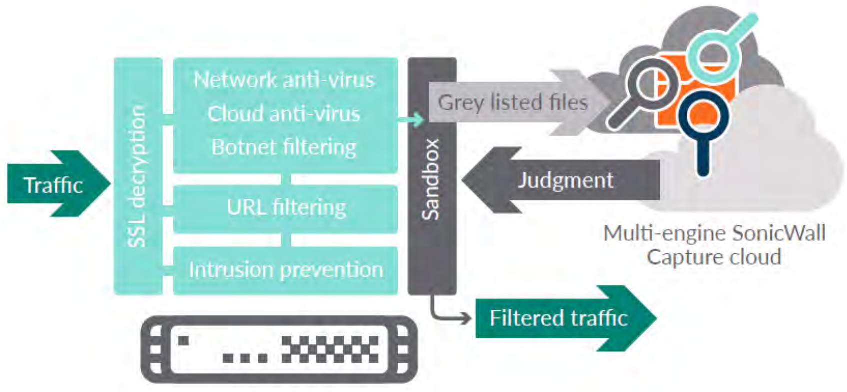
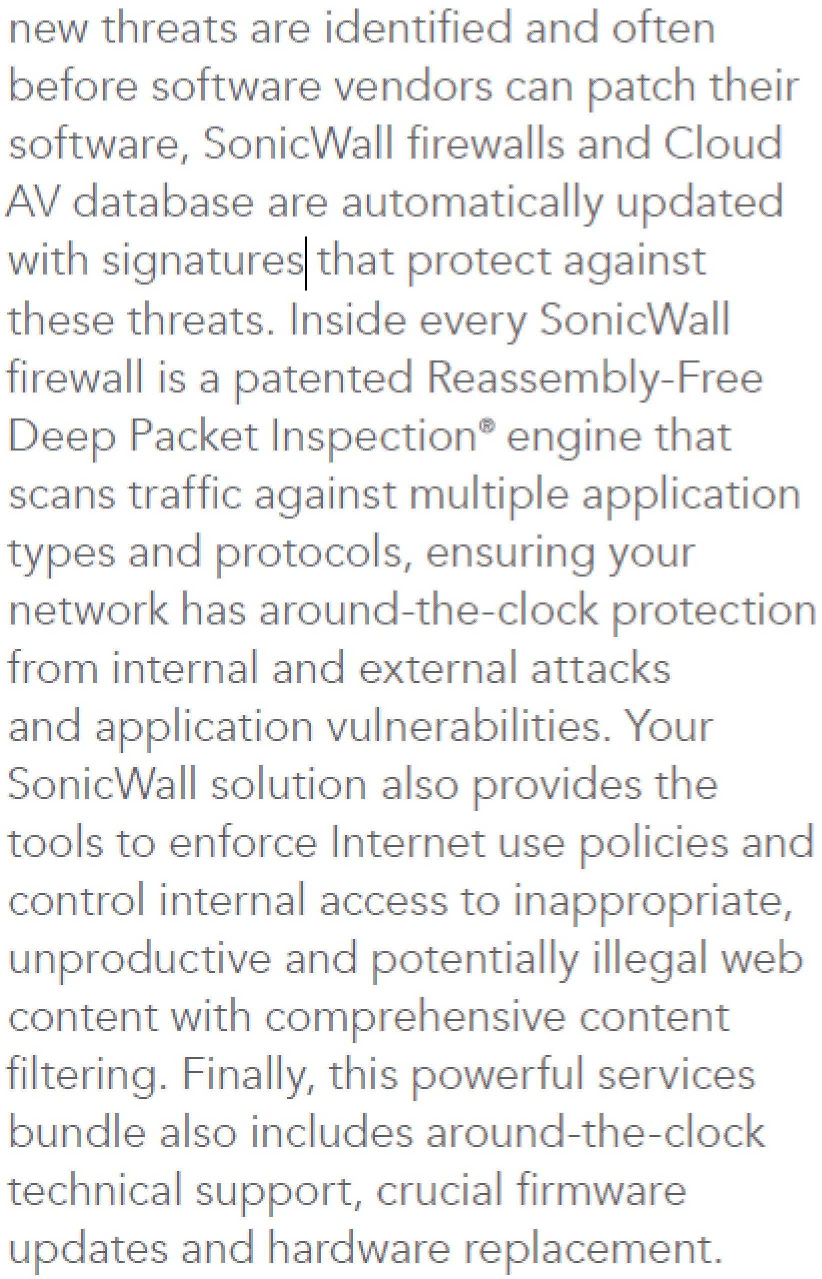
EXHIBIT H

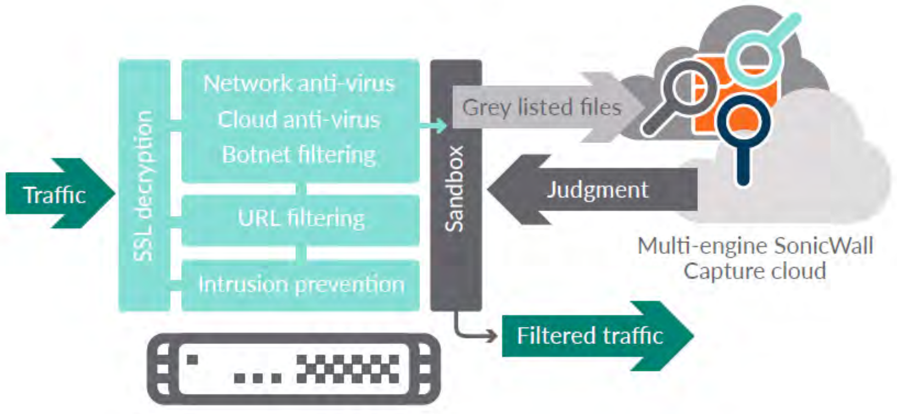
APPENDIX D-2

<table>
<tr><th>6,804,780</th><th>SonicWall Capture Advanced Threat Protection (“ATP”)</th></tr>
<tr><td colspan="2">The statements and documents cited below are based on information available to Finjan, Inc. at the time this chart was created. Finjan reserves its right to supplement this chart as additional information becomes known to it.
For purposes of this chart, “Capture ATP” means Capture Advanced Threat Protection (“ATP”). As identified and described element by element below, Capture ATP infringes at least claims 1, 2, 9, 13, 14, 17, and 18 of the ’780 Patent.</td></tr>
<tr><th>Claim 1</th><th></th></tr>
<tr><td>1a. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:</td><td>Capture ATP meets the recited claim language because it performs a computer-based method for generating a Downloadable ID to identify a Downloadable.
Capture ATP meets the recited claim language because Capture ATP performs a method which generates a Downloadable ID by creating malware attack profiles which include a hash to identify a Downloadable such as malware. The analysis includes scanning the Downloadables which include references to software components required to be executed by the Downloadable (e.g., suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware). Capture ATP uses the Downloadable ID to perform a hash lookup. Capture ATP also meets the claim language because it generates a Downloadable ID for the Downloadable and components of the Downloadable, and then generate a combined Downloadable ID for the Downloadable and the related components.
As shown below, Capture ATP includes both hardware and software components that receive a Downloadable through network traffic and generating a Downloadable ID to identify the Downloadable.


Traffic
SSL decryption
Network anti-virus
Cloud anti-virus
Botnet filtering
URL filtering
Intrusion prevention
Sandbox
Grey listed files
Judgment
Multi-engine SonicWall Capture cloud
Filtered traffic

A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway
FINJAN-SW 007657-60</td></tr>
</table>

	As shown below, Capture ATP generates a Downloadable ID to identify a Downloadable. The Downloadable ID is then provided to other SonicWall Gateways and Cloud AV to protect all SonicWall products.  new threats are identified and often before software vendors can patch their software, SonicWall firewalls and Cloud AV database are automatically updated with signatures that protect against these threats. Inside every SonicWall firewall is a patented Reassembly-Free Deep Packet Inspection® engine that scans traffic against multiple application types and protocols, ensuring your network has around-the-clock protection from internal and external attacks and application vulnerabilities. Your SonicWall solution also provides the tools to enforce Internet use policies and control internal access to inappropriate, unproductive and potentially illegal web content with comprehensive content filtering. Finally, this powerful services bundle also includes around-the-clock technical support, crucial firmware updates and hardware replacement. FINJAN-SW 005949-51
9b. a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the	Capture ATP meets the recited claim language because it provides a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable. Capture ATP meets the recited claim language because Capture ATP includes software components or proxy software that is a communications engine that

Downloadable; and	obtains suspicious traffic flows for analysis through an application program interface, and the content in these traffic flows include Downloadables such as web page and/or email attachments. These Downloadables include references to software components required to be executed by the Downloadable (e.g. suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware). Downloadables that include one or more references to software components required to be executed by the Downloadable include a web page that includes references to JavaScript, visual basic script, ActiveX, injected iframes, and a PDF that includes references to JavaScript, swf files or other executables. Typically, SonicWall characterizes them as drive-by-downloads or droppers as such Downloadables are usually programmed to take advantage of a browser, application, or OS that is out of date and has a security flaw. The initial downloaded code is often small enough that it wouldn't be noticed, since its job is often simply to contact another computer where it can pull down the rest of the code on to the computer. In particular, such software components are usually programmed to be downloaded and run in the background in a manner that is invisible to the user and without the user taking any conscious actions as just the act of viewing a web-page that harbors this malicious code is typically enough for the download and execution to occur. Capture ATP includes a communications engine to obtain and scan Downloadables that may include malware embedded in images, JavaScript, text, and Flash files. As shown below, Capture ATP obtains and conducts analysis on Downloadables such as Executable files (e.g., PE, Mach-O, DMG, bin, .com, .dat, .exe, .msi, .msm, .mst) PDF files, Java (e.g., .class, .ear, .jar, .war), MS Office file types, Flash and Silverlight applications, Script files, and installer files through an application program interface.  Traffic SSL decryption Network anti-virus Cloud anti-virus Botnet filtering URL filtering Intrusion prevention Sandbox Grey listed files Judgment Multi-engine SonicWall Capture cloud Filtered traffic *A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway* FINJAN-SW 007657-60 As shown below, Capture ATP includes a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable. Capture ATP analysis files

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.