EXHIBIT 2

Trials@uspto.gov
571-272-7822

Paper 7
Date: March 23, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner

Case IPR2015-02000
Patent 7,418,731

Before THOMAS L. GIANNETTI, MIRIAM L. QUINN, and PATRICK M. BOUCHER, *Administrative Patent Judges.*

GIANNETTI, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Palo Alto Networks, Inc. ("Petitioner") filed a Petition pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–22 (all claims) of U.S. Patent No 7,418,731 (Ex. 1001, "the '731 patent"). Paper 1 ("Pet."). Finjan, Inc. ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp."). Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we deny Petitioner's request and deny institution of an *inter partes* review of all challenged claims.

I. BACKGROUND

A. The '731 Patent (Ex. 1001)

The '731 patent is titled "Method and System for Caching at Secure Gateways." Petitioner summarizes the patent as follows:

> The '731 patent is directed at preventing the spread of viruses in and among computer networks. The '731 patent discloses gateways and methods of operating gateways that scan incoming or outgoing files for viruses and store the scanned files in a file cache. The gateways also store security profiles, which are lists of the operations that the scanned files are programmed to perform, and, in some cases, security policies for the intranet computers connected to the gateway.

Pet. 1.

The invention is illustrated by Figure 1 of the patent, reproduced here:

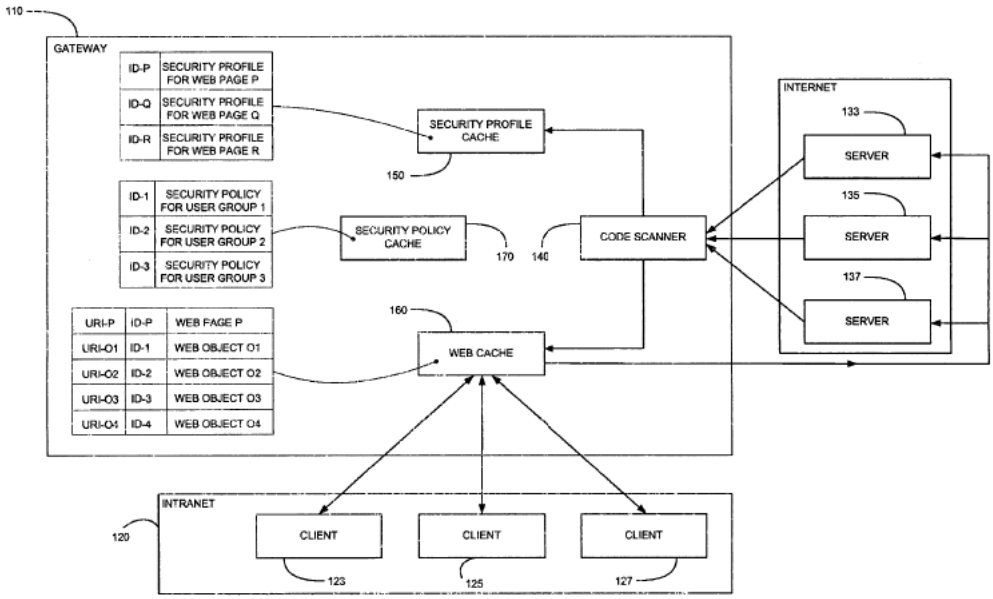

FIG. 1

Figure 1 is a simplified block diagram of a network gateway in accordance with the '731 patent. Ex. 1001, col. 5, ll. 22–24. Shown in Figure 1 is network gateway computer 110, which serves as a proxy between an intranet and the Internet. Specifically, gateway computer 110 intervenes between requests for web pages originating from intranet 120 of clients 123, 125, and 127, and responses originating from Internet servers 133, 135 and 137. *Id.* at col. 5, ll. 24–30.

The gateway computer includes code scanner 140 for scanning incoming web pages and web objects in order to detect the presence of malicious executable scripts or active code. When gateway 110 receives a web page, it also retrieves the web objects referenced by the web page, and scanner 140 scans the web page and the web objects that may be malicious. *Id.* at col. 5, l. 63–col. 6, l. 2. Scanner 140 analyzes each file it scans to determine the nature of computer operations that the file is programmed to

perform, and derives a security profile therefor, summarizing potentially malicious computer operations. *Id.* at col. 6, ll. 17–21. Web page security profiles are stored in a security profile cache 150, and the web page and the web objects that the page references are stored in web cache 160. *Id.* at col. 6, ll. 56–58.

Use of a hash ID for web pages and web objects serves to identify web content duplicates, and to determine if web content on the Internet has changed since it was earlier cached within web content cache 160. *Id.* at col. 7, ll. 18–20.

When a client computer requests a web page, P, from a server computer, the request is first transmitted to gateway computer 110, which checks whether or not the web page is already resident within web cache 160. If not, then the computer gateway forwards the request to the server computer, which in turn sends the requested web page to gateway computer 110. *Id.* at col. 7, ll. 28–35.

Upon receipt of the requested web page P, gateway computer 110 fetches the web objects referenced by the page, determines which files to scan, determines security profiles for the scanned files, caches the security profiles for the web page in security profile cache 150, and caches web page P and web objects in web cache 160. *Id.* at col. 7, ll. 35–42.

After the gateway computer has stored web page P in the web cache, and has stored its corresponding security profile in the security profile cache, it determines whether or not to send the web page to the client computer that requested it. If web page P may perform malicious operations to the client computer, then the gateway computer may not transmit this web page to the

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.