# Tenable and Palo Alto Networks

## Enhance your Perimeter Defenses

## The Challenge

To combat the ever-increasing threat landscape, many organizations have several solutions deployed as a part of their security strategy. This layered approach frequently leads to silos of data with little visibility or context available to inform action. As enterprise firewalls pass traffic, they generate enormous amounts of data for the networking and security teams. With the right analysis, this data becomes a powerful tool to quickly adapt and ensure coverage and visibility into even the most remote corners of the network.

Vulnerabilities and weaknesses can exist anywhere in your infrastructure–including on the hardware that's working to keep your network safe. As a result, monitoring the security settings of enterprise firewalls is critical for maintaining a network's security posture. Both regular audit checks and passive network monitoring are needed to ensure your organization is able to:

- Identify potential security misconfigurations on your Palo Alto firewalls
- Assess remote hosts not present during active scans
- Identify and scan new hosts on remote network segments
- Uncover advanced cyberthreats by correlating firewall log data with log data from other network and security devices

## The Solution

Deploying Tenable™ solutions alongside your Palo Alto Networks devices gives you a comprehensive security and vulnerability management solution. Tenable Nessus not only assesses Palo Alto Networks devices for vulnerabilities, but audits configuration settings against best practices for securing them against attackers. Tenable performs security configuration audits specifically designed for both physical and virtual Palo Alto Networks firewalls, giving you peace of mind that your firewalls will always be in check with the latest best-practice hardening guidelines.

Together with Tenable solutions, the data captured by Palo Alto Networks help you dive deeper into identifying weakness in your environment. Tenable SecurityCenter Continuous View™ is uniquely capable of gathering and analyzing Palo Alto Firewall data to identify assets not active during vulnerability scans, finding unknown assets not catalogued previously, and automatically launching scans to gain visibility into the security of these devices. By combining Palo Alto logs with other security data across your environment, you can identify endpoint threats with behavior monitoring and indicators of compromise through continuous analysis using current threat intelligence.

With Tenable's purpose-built Palo Alto Firewall dashboard, you can easily monitor the configuration and traffic status of your Palo Alto firewall(s) and correlate firewall log data with other security data to discover unknown assets, indicators of a vulnerability and suspicious user behavior, in a single location and without requiring firewall management privileges.

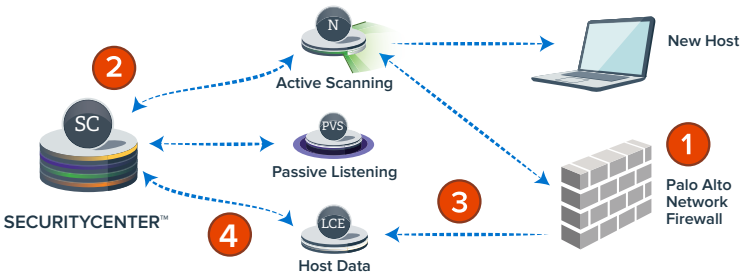
### Benefits

- **Reduce your attack surface** ensuring your firewalls are configured to Palo Alto Networks best practices
- **Monitor configuration and traffic status** from a single pane of glass, without requiring firewall management privileges
- **Uncover advanced cyberthreats** by correlating Palo Alto firewall log data with log data from other network and security devices
- **Discover vulnerabilities and misconfigurations** of mobile devices and virtual machines not present during your last full-network scan

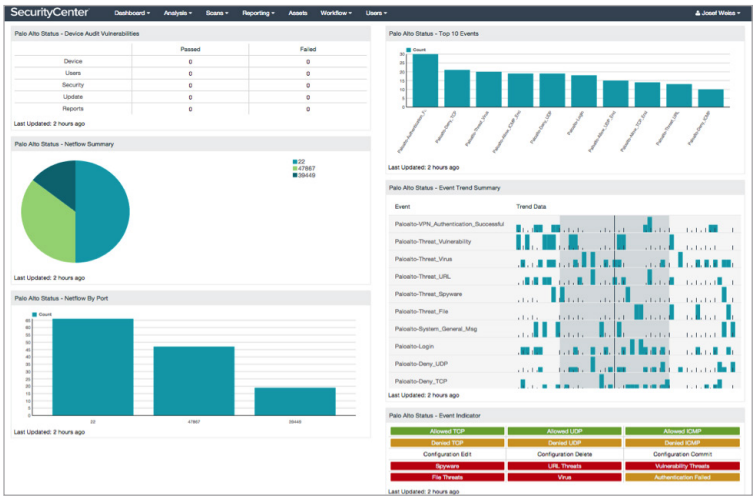
### Components

- Tenable Nessus®
- Tenable SecurityCenter Continuous View
- Palo Alto Networks firewall
- Palo Alto Networks XML API

## How It Works




1. Tenable initiates a credentialed scan of the Palo Alto firewall, authenticating credentials via the Palo Alto XML API.
2. Any detected Palo Alto firewall security misconfigurations can be reviewed within Tenable dashboards and reports.
3. The Palo Alto firewall exports log data in real-time to Tenable, then never-before-seen hosts are added to dynamic asset lists, thus triggering active scans.
4. Tenable combines log data from the Palo Alto firewall with other security and network log sources to uncover hidden cyberthreats.




*The Tenable Palo Alto Firewall dashboard enables security administrators to view a summary status of firewall information and includes indicators for events, configuration audits, and NetFlow statistical graphs in a single location.*

The combination of Tenable and Palo Alto Networks gives you a complete view of your network security posture. Maximize your investment in Palo Alto Networks and get the most comprehensive security in the industry by integrating Tenable and Palo Alto Networks. To learn more about Tenable's solutions visit tenable.com

## About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyber threat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at paloaltonetworks.com.

## About Tenable

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

tenable® network security

**For More Information:** Please visit tenable.com
**Contact Us:** Please email us at sales@tenable.com or visit tenable.com/contact