Palo Alto Networks and Tenable

Protecting Industrial Control Systems and Critical Infrastructure

Benefits of the Integration

- Get an in-depth view of external and internal threats targeting OT environments that can be addressed via firewall rules.
- Take advantage of automated asset discovery, classification, and tracking, facilitating better firewall management.
- Address regulatory compliance and change management requirements.

The Challenge

Industrial control system (ICS) networks lack visibility and security controls. With the rise of external and internal threats targeting operational technology (OT) infrastructure, there is a need for an approach that provides real-time visibility and security while addressing the unique technical and operational requirements of these networks. Having these OT alerts separate from existing IT procedures and policies creates additional challenges in the remediation and implementation of rules for improved security protections.

Tenable.ot (Powered by Indegy)

Tenable.ot (powered by Indegy) is based on proprietary, patent-pending technologies developed by ICS security experts. It is purpose-built to provide real-time threat detection and mitigation, asset tracking, vulnerability and configuration management, and visibility for ICS networks. Whether a threat is "external-in," an insider attack, or a misconfiguration, the product captures all changes and provides detailed alerts, enabling security staff and control engineers to quickly pinpoint the source of the problem.

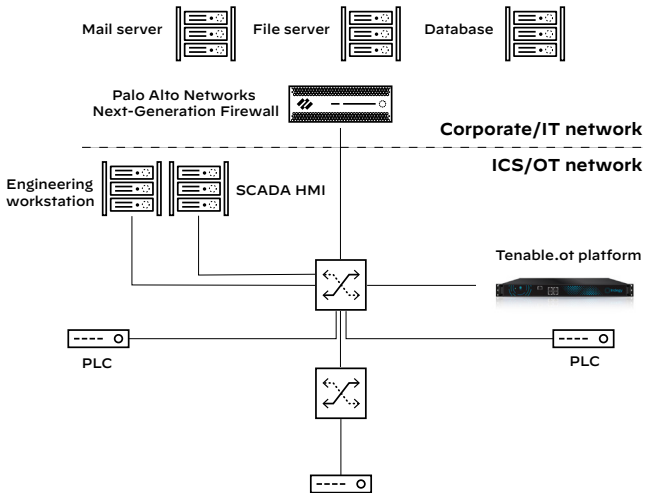

Figure 1: Palo Alto Networks and Tenable securing IT/OT environments

Tenable.ot is an all-in-one turnkey appliance that offers:

- **Device integrity**: Using native protocols, the system queries devices for full configuration and state in addition to detecting local changes to provide extra context when there are alerts.
- **Policy-based detection**: Behavioral analysis detects critical changes that may not rise above the statistical noise. Tenable.ot also has capabilities for granular use of allow and block lists as well as triggering of device integrity checks for predetermined scenarios.
- **Anomaly detection**: The system highlights traffic that falls outside the baseline.

Palo Alto Networks

Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

ML-Powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. You can align security with your business policies as well as write rules that are easy to understand and maintain. The NGFWs have been globally deployed in multiple critical infrastructure sectors, including utilities and transportation, oil and gas, and manufacturing, to prevent successful cyberattacks on ICS and SCADA.

Palo Alto Networks & Tenable

Palo Alto Networks and Tenable have partnered to provide customers with a seamless offering to increase visibility into ICS and critical infrastructure as well as protect them from cyberthreats. Tenable's advanced, ICS-specific asset discovery and tracking capabilities integrate with Palo Alto Networks NGFWs via Dynamic Address Group (DAG) technology. DAGs dynamically populate with assets based on tags, which allows Tenable.ot to provide continuous updates on the assets it identifies in an ICS network to help firewall administrators improve the overall cybersecurity posture.

Tenable provides detailed information on each discovered asset, such as IP address, device type, vendor, and model, and delivers it to the NGFW. Taking this data into account, administrators can take advantage of this integration to extend policies across IT and OT environments.

Use Case No. 1: Secure Access to Critical ICS Assets

Challenge

Maintain strict security polices while still allowing critical operational maintenance activities that require network connections to be made to sensitive devices. NGFW administrators face the challenge of effectively managing access—and approving or revoking it on short notice—without having detailed asset inventories or clear visibility into their ICS networks.

Answer

With the integration of Tenable.ot and Palo Alto Networks NGFWs, administrators can now easily make changes to rules and gain complete access control over ICS networks through the use of DAGs. Administrators can configure rules that apply to specific assets, taking their various characteristics into account. For example, when access to the ICS network is required only to update Siemens engineering stations, the NGFW administrator can set a rule that applies only to these devices without relying on manual mapping based on IP addresses, which can constantly change.

Use Case No. 2: Secure Network Connections Between ICS and IT Environments

Challenge

Facilitate secured network connections between assets in the ICS network and IT applications that reside on the corporate network. Firewall administrators are currently forced to set permanent firewall rules that are too permissive and can't automatically adapt when changes occur. This increases security risk by expanding the potential attack surface.

Answer

The integration of Tenable.ot and Palo Alto Networks NGFWs lets administrators use DAGs to configure rules addressing individual ICS assets and groups by type. There is no need for prior knowledge of the network or address specifics. For example, an administrator can set a rule to allow only necessary communications to facilitate data gathering by a manufacturing efficiency system.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
palo-alto-networks-and-tenable-tpb-061720