TECHNICAL SOLUTION BRIEF

Protecting your critical infrastructure control systems

Discover how machine-learning powered threat prevention from Palo Alto Networks hosted on rugged communications hardware can improve the availability and reliability of your industrial control systems.

SIEMENS

Introduction

Industrial control systems in critical infrastructures, for example, in electric power and transportation industries, are undergoing rapid digitalization. This increasing convergence of OT and IT systems puts a higher demand on network reliability and performance. Furthermore, cyberattacks on OT networks have become increasingly sophisticated with the potential for severe damage. The need of the hour is to smoothly and effectively secure both legacy and modern control systems. To ensure holistic security and business continuity, industrial network owners can look to integrated cybersecurity solutions.

Contents

Protecting industrial control systems

Industrial control systems require enhanced reliability to support purpose-built applications in locations with harsh conditions, such as extreme temperatures and a high level of EMI (electromagnetic interference). Delivering solutions that meet the cybersecurity compliance requirements set for mission-critical applications in these demanding environments is a significant challenge for operators of critical infrastructure. The frequency and complexity of cyberattacks targeting utilities, energy pipeline operators, manufacturers, and other organizations that operate critical infrastructure are increasing. Every aspect of security, from industrial control systems to physical security, must be integrated to provide security teams with centralized visibility and control to protect critical infrastructure.

We have partnered with Palo Alto Networks (PANW) to integrate the PANW VM-Series Virtual Next-Generation Firewalls (NGFWs) and the RUGGEDCOM Multi-Service Platforms (rugged layer 3 networking devices with computing capabilities) to enable continuous scalable hardware that will allow network owners to extend consistent security policy and visibility across IT, critical OT, and industrial control systems (ICS) infrastructure.

Benefits of the integration

Palo Alto Networks VM-Series Virtual NGFWs deployed with full capabilities on the modular RUGGEDCOM RX1500 series Multi-Service Platforms with the RUGGEDCOM APE1808 industrial application processing engine offer multiple benefits to organizations:

- Integrated hardware and software solution with a small physical footprint from a single, trusted source
- Eliminates the costs and complications of installing an external industrial PC for most industrial deployment scenarios
- Blocks malware and performs application control
- Provides Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for encrypted traffic
- Detects and prevents advanced attacks inline and within application flows in the network

The integration

RUGGEDCOM RX1500 series
The RUGGEDCOM RX1500 series Multi-Service Platforms are managed, modular, and field-replaceable networking devices that ensure reliable connectivity for mission-critical applications in harsh industrial environments. They are certified to operate between temperature extremes of -40 °C and 85 °C and demonstrate a high level of immunity to EMI, shock, and vibrations. In addition, they support switching, routing, IPsec (VPN), and stateful firewall functions and ensure data security at the local area network (LAN). The RUGGEDCOM APE1808 is a powerful industrial application hosting platform and a line module for RUGGEDCOM RX1500 series devices. Based on Intel Quad Core x86_64 architecture, the APE provides a standards-based platform to deploy commercially available software applications at the network edge for electric power, transportation, oil and gas, and other critical infrastructure industries.

Palo Alto Networks VM-Series Virtual NGFWs
Palo Alto Networks VM-Series Virtual Next-Generation Firewalls consistently protect public and private clouds, virtualized data centers, and branch environments by delivering inline network security and threat prevention. The VM-Series virtual firewall embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts – going beyond intrusion prevention system (IPS) technologies to prevent all known threats across all traffic in a single pass without sacrificing performance. It's also easy to add subscriptions, like Data Loss Prevention (DLP) and IoT (Internet of Things) Security. The VM form factor makes it ideal for deployment in environments where it is difficult or impossible to install a hardware firewall. VM-Series firewalls also provide on-demand scalability and the ability to integrate security provisioning directly into your DevOps workflows and CI/CD pipeline. Panorama™ network security management provides easy-to-implement, consolidated policy creation in a centralized management platform in the control center. This ensures effective security and simplifies compliance without slowing down your business, even in dynamic environments.

Palo Alto Networks and RUGGEDCOM APE1808
Integration of Palo Alto Networks VM-Series Virtual NGFWs on our RUGGEDCOM APE1808 module helps you protect critical IoT infrastructure from advanced cyberthreats. The firewalls natively analyze all traffic in a single pass to determine application identity, the content within, and user identity. Machine-learning (ML) capabilities and scalable architecture also help protect industrial systems where RUGGEDCOM RX1500 series Multi-Service Platforms are deployed.
With the APE1808 module plugged into the RUGGEDCOM RX1500 series Multi-Service Platforms, you can protect HMI, engineering workstations, and field devices located at remote sites. The VM-Series Virtual NGFWs serve as a perimeter gateway in these scenarios, providing a secure IPsec VPN termination point and a segmentation gateway that prevents threats from moving from workload to workload. This integrated solution can also be deployed to provide application-level monitoring for control centers running SCADA systems.

paloalto
NETWORKS

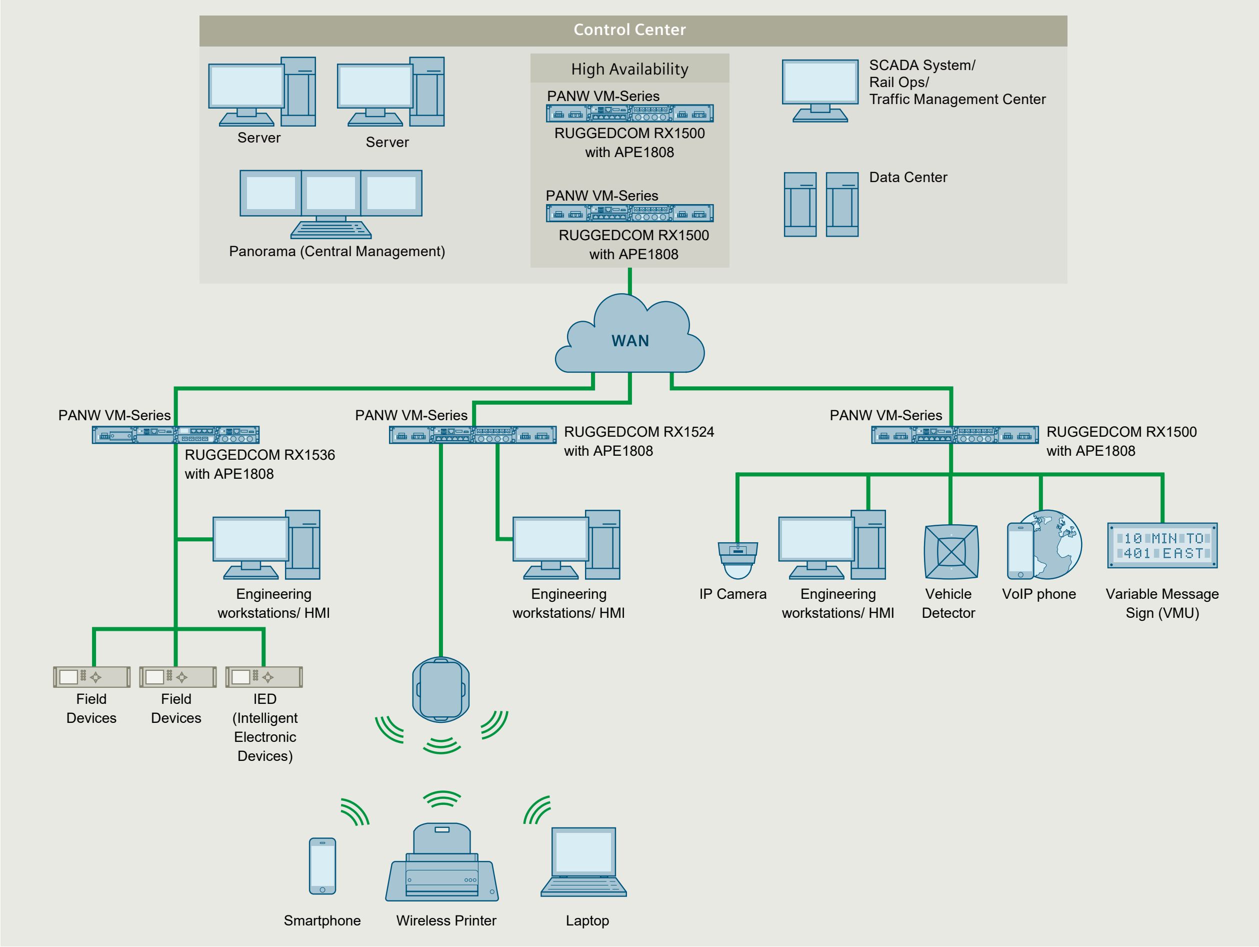
Control Center
Server
Server
Panorama (Central Management)
High Availability
PANW VM-Series
RUGGEDCOM RX1500 with APE1808
PANW VM-Series
RUGGEDCOM RX1500 with APE1808
SCADA System/ Rail Ops/ Traffic Management Center
Data Center
WAN
PANW VM-Series
RUGGEDCOM RX1536 with APE1808
PANW VM-Series
RUGGEDCOM RX1524 with APE1808
PANW VM-Series
RUGGEDCOM RX1500 with APE1808
Engineering workstations/ HMI
Engineering workstations/ HMI
IP Camera
Engineering workstations/ HMI
Vehicle Detector
VoIP phone
10 MIN TO 401 EAST
Variable Message Sign (VMU)
Field Devices
Field Devices
IED (Intelligent Electronic Devices)
Smartphone
Wireless Printer
Laptop

Figure 1: Integration of Palo Alto Networks VM-Series Firewall with RUGGEDCOM RX1500 series Multi-Service Platform and RUGGEDCOM APE

Use case 1: Inline advanced attack prevention for electric utilities

Electric utilities task anomaly intrusion detection with deep packet inspection and visibility on industrial protocols with the ability to detect advanced threats using modern security tools. What's also needed is networking, user and policy lookup, application and decoding, and signature and content matching in a single pass. Furthermore, the ability to extend the security context to include command-and-control attacks as well as block unknown vulnerabilities for electric utilities is becoming more important in today's digital transformations. This is especially relevant in remote locations where secure WAN connectivity back to the SCADA control center over SSL with inspection of IPsec traffic is a must.

Solution

Using the Palo Alto Networks VM-Series Virtual NGFWs on the RUGGEDCOM RX1500 series devices with the APE1808 module to collect and analyze network traffic lets electric utilities perform deep packet inspection across the network. They can also protect SCADA control systems by ensuring secure data transmission and blocking unwanted traffic. The firewalls also help protect critical infrastructure by enabling real-time monitoring and risk. Inline traffic monitoring and alerting occur passively, with task no impact on OT operations.

Use case 2: Secure networks in transportation systems

New attack vectors in transportation systems, including rail (e.g., trackside, wayside, onboard), Intelligent Transportation Systems (ITS), and airports, if left unchecked and unmonitored at the packet level, can lead to catastrophic events. Blocking unwanted traffic, monitoring encrypted traffic, and ensuring uncompromised data is sent back to SCADA systems are essential security measures for this sector. Also critical is using threat prevention, URL filtering, and monitoring all types of data traffic to ensure network segmentation.

Solution

Deploying Palo Alto Networks VM-Series Virtual NGFWs on the RX1500 series with the APE1808 module in wayside cabinets in the rail industry or in field application deployments for ITS makes it possible for security teams to monitor all network activity at the field level. The RUGGEDCOM APE1808 has a small footprint as a cybersecurity solution for space-constrained industrial networks. Security subscriptions, such as Threat Prevention, when enabled, provide consistent and predictable performance. This functionality is extremely important to ensure compliance and safety in real time for public transport systems.

Solution highlights

Next-generation firewall with application control

- Blocks and restricts access to resources
- Granular control using security policies
- Bandwidth optimization
- Visibility and control over network communication
- Full TLS/SSL inspection capabilities

Advanced malware protection

- Real-time malware detection and prevention
- Command and control protection
- Comprehensive botnet and antispam protection
- Continuous signature updates
- Detecting and blocking both malware and vulnerability exploits in a single pass

Threat prevention service

- Built-in IDS/IPS functionality
- Threat detection and prevention
- Real-time threat intelligence
- Stateful pattern matching detects attacks across multiple packets
- Extensive database of IPS signatures

Industrial Security Service

- DPI capability for ICS/SCADA protocols
- Granular control and visibility for ICS/SCADA communication
- Broad support for industrial protocols and applications

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.
To learn more, visit **www.paloaltonetworks.com**

About Siemens Digital Industries

Siemens Digital Industries (DI) is an innovation leader in automation and digitalization. Closely collaborating with partners and customers, DI drives the digital transformation in the process and discrete industries. With its Digital Enterprise portfolio, DI provides companies of all sizes with an end-to-end set of products, solutions, and services to integrate and digitalize the entire value chain. Optimized for the specific needs of each industry, DI's unique portfolio supports customers to achieve greater productivity and flexibility. DI is constantly adding innovations to its portfolio to integrate cutting-edge future technologies. RUGGEDCOM hardware and software products are part of Siemens Digital Industries portfolio. They provide a level of robustness and reliability that have set the standard for communications networks deployed in harsh environments. Siemens Digital Industries has its global headquarters in Nuremberg, Germany, and has around 76,000 employees internationally. For more information, visit **www.siemens.com/ruggedcom/cybersecurity**

For more information, please visit:
siemens.com/ruggedcom

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

Siemens Canada Limited
300 Applewood Crescent
Concord, Ontario, L4K 5C7
Canada

Subject to change without prior notice
Article No. 6ZB5531-0BD01-0BA0
Dispo 26000
BR 0522 0 PoD 8 En
Printed in Germany

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit: **siemens.com/industrialsecurity**

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under: **siemens.com/industrialsecurity**

The information provided in this brochure contains descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice. All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.