SIEMENS

Palo Alto Networks VM-Series Firewalls and RUGGEDCOM Multi-Service Platforms

Rugged Network Components from Siemens for Harsh Environments with a Built-in Security Platform

Benefits of the Integration

Palo Alto Networks VM-Series Virtual NGFWs deployed with full capabilities on the modular RUGGEDCOM RX1500 series with the RUGGEDCOM APE1808 application processing engine from Siemens help your organization protect critical infrastructure by:

- Offering an integrated hardware and software solution with a small physical footprint from a single, trusted source
- Eliminating the costs and complications of installing an external industrial PC for most industrial deployment scenarios
- Blocking malware and performing application control
- Providing Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for encrypted traffic
- Detecting and preventing advanced attacks inline and within application flows in the network

The Challenge

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 rising. 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.

RUGGEDCOM, Network Components from Siemens for Harsh Environments

RUGGEDCOM RX1500 series Multi-Service Platforms are managed, modular, and field-replaceable networking devices that ensure reliable connectivity for mission-critical applications. They are certified to operate between temperature extremes of -40° to 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

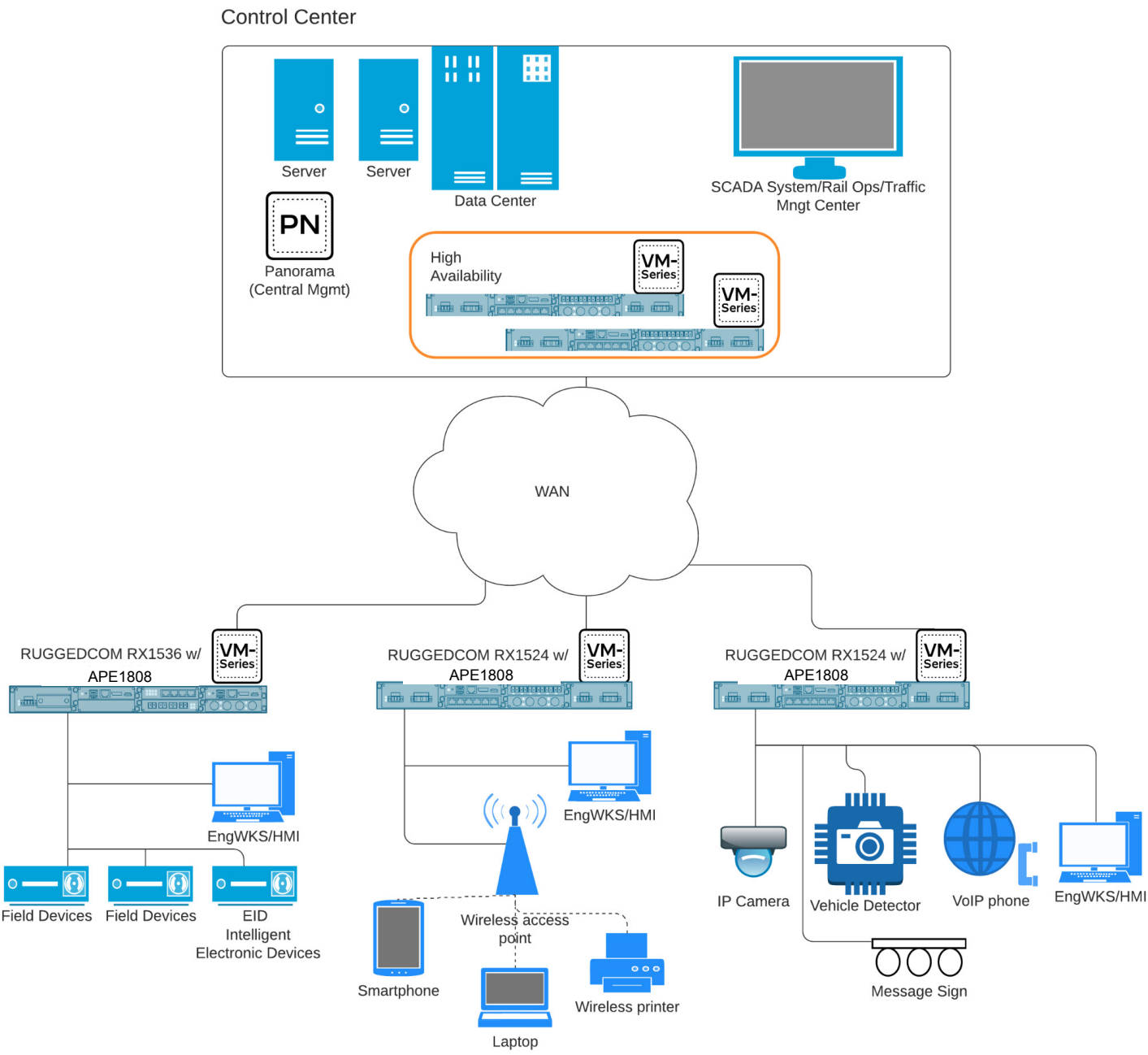

Figure 1: Virtual NGFW general architecture

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 NGFWs on the RUGGEDCOM APE1808 module from Siemens 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 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 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.

Use Case 1: Inline Advanced Attack Prevention for Electric Utilities

Challenge

Electric utilities seek anomaly intrusion detection with deep packet inspection and visibility into 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. Further, 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 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 no impact on OT operations.

Use Case 2: Secure Networks in Transportation Systems

Challenge

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 systems that transport people.

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. To learn more, visit www.siemens.com.

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 | SIEMENS

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