VM-Series Virtual Next-Generation Firewall and iS5 Communications RAPTOR

Purpose-Built Critical Infrastructure Networking Platform

Benefits of the Integration

- Purpose-built substation-grade hardware certified to IEC 61850-3 and IEEE 1613.
- Integrated best-in-class hardware and software.
- Small physical footprint with rackmount or DIN rail options.
- Increased visibility into ingress/egress traffic.
- The ability to implement least-privileged access by zone or even by the individual device.
- Consistent threat protection across zones.
- Customized protection on a per-zone basis.

The Challenge

Industrial control systems and operational technology (OT) networks are increasingly under attack from a wide range of bad actors. Due to digitization, the need for connectivity to these networks has exposed these systems to threats. In response, operators have deployed a wide range of cybersecurity devices, including next-generation firewalls (NGFWs) with deep packet inspection of OT protocols. The use of best-in-class solutions for various network and security components provides good network security. Still, the side effect of these implementations is the proliferation of specialized boxes, causing siloed data and increased management and maintenance costs. These devices occupy valuable rack space, require recabling of the network, and can introduce additional points of failure. Furthermore, many cybersecurity devices used were not engineered to meet the demanding environmental requirements, such as IEC 61850-3, for electric substations or support high-voltage DC power supplies.

The Solution

The deployment of a multiservice networking platform with integrated general-purpose computing capability can permit the integration of advanced cybersecurity functions in virtual machines running right on the network switch or router. The switch may be configured to place the cybersecurity function at the right location within the network topology, which for an NGFW, is generally inline between the LAN and WAN interfaces. This approach eliminates separate boxes and their associated power supplies and greatly simplifies overall wiring. The use of hardware platforms specifically built for these environments allows simple deployment and ensures long mean time between failures (MTBF).

iS5 Communications RAPTOR

The RAPTOR is an intelligent cybersecure networking platform built specifically for the harsh environments found in electric substations and other industrial facilities. It has the highest performance in the industry with 64 Gb/s full line speed and 4X 10 Gb/s + 24 1 Gb/s ports or up to 32 ports overall. The iBiome OS is an all-encompassing operating system that supports L2/L3 switching and routing on a single platform. Its modular system of field-replaceable modules, redundant hot swappable power supplies, and ability to run third-party software applications make it a very flexible platform for today and the future. Line modules exist for copper Ethernet and SFPs, which support a wide range of fiber optic options, serial interfaces, and HSR/PRP for zero failover time redundancy. IEEE 1588 Precision Timing Protocol is supported, and Power over Ethernet (PoE) is available as an option. Rackmount and DIN rail-mounting options are available.

Palo Alto Networks VM-Series Virtual Next-Generation Firewall

The Palo Alto Networks VM-Series virtual firewall consistently protects public and private clouds, virtualized data centers, and branch environments by delivering inline network security and threat prevention. Public cloud platforms and software-defined network solutions lack the threat prevention capabilities needed to keep your environment safe. VM-Series virtual firewalls augment your security posture with the industry-leading threat prevention capabilities of the Palo Alto Networks NGFW in a VM form factor, making it automatable, scalable, and easily deployed.

Palo Alto Networks and iS5 Communications RAPTOR

The integration of the Palo Alto Networks virtual firewall on the iS5 RAPTOR helps protect ICS, SCADA, and IoT networks in a range of critical infrastructure industries. It provides improved visibility of assets, network traffic, and risks, and its deep packet inspection technology provides intuitive, actionable intelligence about network traffic. Along with the iS5 Communications RAPTOR, the Palo Alto Networks virtual NGFW creates a highly secure gateway device, protecting the HMIs, workstations, and field devices in the facility while supporting secure VPN or SD-WAN connectivity to the control center or enterprise.

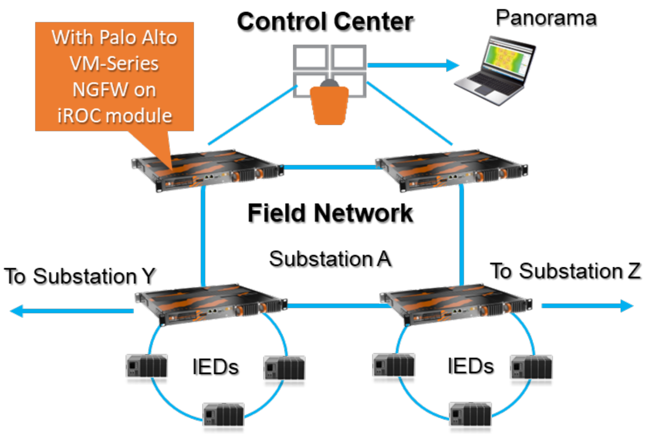

Figure 1: iS5 and Palo Alto Networks integration

Use Case 1: Advanced Cybersecurity for Electric Substations

Challenge

Electric utilities need strong cybersecurity in substations to protect the control systems that manage the flow of electricity in the grid. These control systems are critical infrastructure that, if compromised, could potentially disrupt the power supply or even damage equipment. Advanced cybersecurity measures are required to secure substation networks from unauthorized access to the control systems and ensure their reliability and availability. These cybersecurity measures must be built to withstand the rigors of the harsh substation environment, fit within limited available rack space, and be easy to maintain in distributed remote locations.

Solution

The Palo Alto Networks virtual NGFW delivers advanced security features such as deep packet inspection and application-level filtering to provide highly granular control over network traffic to protect against a wide range of threats. Integrating the VM-Series virtual NGFW as a virtual machine running on the iS5 RAPTOR creates a reliable, compact, and highly sophisticated system at the substation access point. It combines high-performance L2/L3 networking with fine-grained least-privileged access control and deep packet inspection of the control protocols, in a single rack unit or DIN rail-mounted system, with redundant power supplies and which meets the rigorous requirements of IEC 61850-3.

Use Case 2: Unified Cybersecurity Across IT and OT

Challenge

Operators of critical infrastructure need to manage both IT and OT environments and ensure both are safe from a wide range of cybersecurity threats. Having a unified approach across both environments brings numerous benefits, including a consistent and comprehensive approach across both domains, simplified management, and a single point of visibility into the security posture of both the IT and OT environments. This is challenging to achieve due to the harsh physical environment, limited physical space, and specialized operating requirements in an OT installation.

Solution

Enterprises benefitting from the Palo Alto Networks product portfolio in their enterprise networks can expand this into remote sites running the iS5 RAPTOR or MicroRAPTOR in their OT networks. The RAPTOR and MicroRAPTOR are widely recognized for their reliability and robustness in harsh industrial environments, and their functionality is optimized for OT environments. Their ability to support the VM-Series virtual NGFW from Palo Alto Networks allows this functionality to be deployed into the OT networks without requiring additional hardware, enabling a unified cybersecurity approach across the IT and OT assets of the entire enterprise.

About iS5 Communications

iS5 Communications Inc. ("iS5Com") is a global provider of integrated services and solutions, and manufacturer of intelligent Industrial Ethernet products. Our products are designed to meet the stringent demand requirements of utility substations, roadside transportation, rail, and industrial applications. iS5Com's services and products are key enablers of advanced technology implementation such as the Smart Grid, Intelligent Transportation Systems, Intelligent Oil Field, and Internet of Things. All products have the ability to transmit data efficiently without the loss of any packets under harsh environments and EMI conditions. Visit is5com.com to learn more.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.

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