Palo Alto Networks and ZEDEDA

Simplified Deployment and Management of Network Capabilities Within Edge Environments

Key Benefits

- Global edge management and orchestration with a single dashboard across deployments.
- Easy deployment and management of VNFs on a wide range of edge devices for efficient scaling of network capabilities.
- Increased security offered by the combination of Palo Alto Networks advanced security and ZEDEDA's Zero Trust security.
- Comprehensive security framework and consistent security policy enforcement across your edge infrastructure.

The Challenge

As IoT and edge systems grow more interconnected, the issues of security and complexity are becoming increasingly evident. Organizations face a new set of challenges as they extend their security infrastructure to a distributed environment that has no perimeter, is heterogeneous, encompasses devices that may be too constrained to run traditional security tools, and operates at a scale that may run into tens of thousands or more. Deploying security and network functionality efficiently in distributed environments while safeguarding both legacy and modern IoT and edge devices is a demanding and time-intensive process.

The Solution

A centralized, integrated edge computing solution addresses these challenges, enabling easy deployment and management of security capabilities alongside other applications, without requiring separate hardware or management tools. This functionality, coupled with an open architecture built for distributed environments, ensures that IT has the centralized visibility and control necessary over all edge assets, providing confidence that the entire software stack can be trusted, as well as the extensibility required as deployments grow.

ZEDEDA

ZEDEDA delivers an open, distributed, cloud-native edge management and orchestration solution, simplifying the security and remote management of edge infrastructure and applications at scale. ZEDEDA leverages an open architecture built on EVE-OS, allowing any application to be deployed. EVE-OS delivers an industry-leading identity and software attestation workflow that helps ensure the device can be trusted and that the entire software stack deploys consistently.

Palo Alto Networks VM-Series

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. Public cloud platforms and software-defined network solutions provide basic security functionality that lacks the advanced 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 Next-Generation Firewall in a VM form factor, making it ideal for deployment in environments where it's difficult or impossible to install a hardware firewall.

Palo Alto Networks and ZEDEDA

Together, Palo Alto Networks and ZEDEDA provide a unified edge security solution for distributed edge environments. The ZEDEDA edge computing platform, in combination with Palo Alto Networks security tools, enables organizations to

efficiently deploy, secure, and manage their edge computing workloads without requiring additional infrastructure or on-site IT staff.

Use Case 1: Security Management Complexity for Large IoT/OT Deployments

Challenge

The absence of standard security protocols and practices across IoT/OT devices and systems can lead to security vulnerabilities and inconsistencies. Many OT devices rely on legacy systems, making them vulnerable to threats. Limited visibility into IoT and OT devices and activities, coupled with insufficient control mechanisms, can make it challenging to detect and respond to security incidents.

Solution

Palo Alto Networks VM-Series virtual firewalls deployed on the ZEDEDA edge computing platform protect inbound and outbound traffic, allowing deep packet inspection of network traffic for the IoT/OT deployment. Being at the edge, VM-Series virtual firewalls provide real-time monitoring and threat detection for network traffic. The inline traffic inspection prevents impact to OT operations and helps secure the vulnerable legacy systems from hackers. VM-Series virtual firewalls with Threat Prevention and IoT Security subscriptions provide visibility into IoT and OT devices, minimizing the risk of security incidents.

Use Case 2: Segmentation Between Environments

Challenge

Inadequate network segmentation in IoT/OT deployments can result in a larger attack surface, allowing threats to spread across networks. Some IoT/OT devices use insecure communication protocols and channels that can be exploited by attackers to intercept data or launch unauthorized access attempts. Malicious or negligent acts by staff, contractors, or vendors can pose significant security risks.

Solution

Deploying Palo Alto Networks VM-Series virtual firewalls to leverage zone-based policies to segment deployments can help limit attack surfaces, reducing the potential impact of a security breach. VM-Series virtual firewalls inspect east-west traffic to prevent the lateral spread of threats. In the event of a security incident in one segment, network segmentation limits the impact by preventing the spread of threats to other parts of the network and enables more targeted security controls and monitoring. By creating distinct segments of network traffic, organizations can prioritize traffic based on specific requirements, helping ensure optimal performance for critical applications and services.

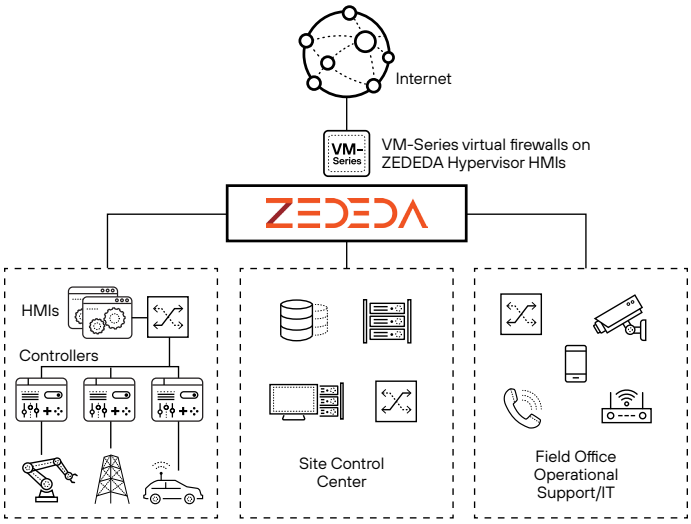

Figure 1: ZEDEDA Hypervisor and Palo Alto Networks VM-Series virtual firewalls integration

About ZEDEDA

ZEDEDA makes edge computing effortless, open, and intrinsically secure—extending the cloud experience to the edge. It reduces the cost of managing and orchestrating distributed edge infrastructure and applications while increasing visibility, security, and control. ZEDEDA delivers instant time to value, has tens of thousands of nodes under management, and is backed by world-class investors with teams in the United States, Germany, and India. For more information, visit www.ZEDEDA.com.

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security, and security operations. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS | ZEDEDA

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

parent_pb_zededa_121824