Solution Brief

Network Security for Edge Computing

Significantly Improve Edge Cloud Security and Efficiency

Improve edge security and reduce latency with Palo Alto Networks' VM-Series virtual firewall and the Intel® Smart Edge platform for healthcare, industrial, and federal government sectors

"It's not possible to account for every threat that a customer may encounter, including very dedicated, well-resourced threats. So it's important for platform and edge cloud security to be as robust as possible."

—Bob Ghaffari, general manager of the Enterprise and Cloud Network Division (ECND) within the Intel Network and Edge Group

Digital transformation has accelerated the drive toward cloud computing technologies and 5G capabilities and the growing demand for near-real-time data flows and content. At the same time, these advancements have created a need for low-latency cloud computing and localized security at the edge of a company's network.

But along with these advancements come challenges. Networks are becoming more complex for both customers and service providers. There are delays in communications and performance. Gaps in security are being discovered along with greater attack surfaces from connected devices and apps.

The healthcare, industrial, and federal government sectors are examining the possibilities and preparing for these new business models.

- Healthcare is looking to implement technology-driven treatments. Their goal is to help improve the patient experience, quality of care, and emergency services. They also expect to reduce costs.
- Industrial needs wireless communication between devices. Sensors and robots are required to automate production lines, enhance productivity, and increase safety.
- Federal government wants stronger and faster connectivity. They need to enable applications at the edge of the network that rely heavily on mobile devices. It's crucial that the connections are secure and reliable across the harshest environments, including natural disasters.

Organizations are implementing 5G to create a fully mobile, connected ecosystem. They need significantly faster data speeds, reliable low latency, and better support for new edge-native applications. Cloud servers at the edge extend data processing closer to the data sources and the user.

Challenge: Edge servers can be complex and create gaps in security with cloud computing and 5G at the network edge

To deliver cloud computing and 5G capabilities at the network edge, IT departments are deploying multi-access edge computing (MEC) servers. However, using MEC servers can result in communication gaps over networks. It can also open up advanced security risks, leaving security teams scrambling to respond to quickly moving attacks while using manual processes.

Fortunately, to help simplify this process—and enhance edge cloud security and performance—Intel has developed Intel® Smart Edge software for open and commercial MEC environments.

Traditional MEC solutions require significant systems integration. They leverage multiple technologies and products, creating a complex user experience for both the customer and the service provider.

However, Intel Smart Edge provides a simpler integrated platform. It takes advantage of Intel® Xeon® processor-based servers, accelerators, and platform security technologies. This solution supports a wide range of use cases without rewriting software. Intel Smart Edge provides the low latency, simplicity, and open architecture that organizations need to roll out LTE, 5G, or Wi-Fi connectivity.

Security is a critical issue. Organizations must effectively address security gaps and fast-moving attacks as the number of devices and data on their network grows exponentially. MEC servers that deliver cloud computing and 5G are located at the edge of a company's network. The boundaries are not protected, which leaves sensitive data highly vulnerable to security threats.

Solution: Intelligent MEC security with Palo Alto Networks' VM-Series virtual firewall and Intel Smart Edge

When it comes to security, every second matters. Millions of new malware samples are being identified along with thousands of new malicious websites generated daily. Modern malware can infect thousands of systems within seconds before protective measures can be developed and deployed.

Intel Smart Edge offers a number of powerful, integrated security features. But it takes it one step further with machine learning. Intel has combined forces with Palo Alto Networks to pair the Intel Smart Edge with the VM-Series virtual firewall.

The solution uses a zero-trust model for all connections, users, applications, and microservices. It reduces attacks while detecting and blocking known and unknown threats on all ports. It also employs a defense-in-depth strategy that constantly operates in an assumed hostile environment. A layered defense helps ensure a strong baseline of security.

Organizations can significantly increase security for their MEC servers supporting private 5G, LTE, or Wi-Fi networks and on-premises applications. This strategy provides peace of mind for the enterprise and the operator that their edge applications are protected.

The six main protection layers

1. Cryptographic verification

A malicious service cannot impersonate another service or replay prior requests without undergoing a verification. It must prove its identity to further reduce risks by using cryptographic keys and exchange of certificates.

2. Trusted Platform Model 2.0 (TPM 2.0)

TPM is a microcontroller that stores keys, passwords, digital certificates, and other secrets. It can be used to authenticate and verify the integrity of the platform.

3. Public key infrastructures (PKI)

PKIs are commonly avoided and often improperly implemented. The Intel® Smart Edge simplifies PKI issues for users to the point where they can become completely transparent.

4. Service chaining

Service chaining manages networks by automating traffic flow between multiple services. It also optimizes the use of network resources to improve performance of applications. The VM-Series firewall can be inserted within the service chain to ensure security is inspected for all flows. It can also be used for a specific traffic flow.

5. Application threats

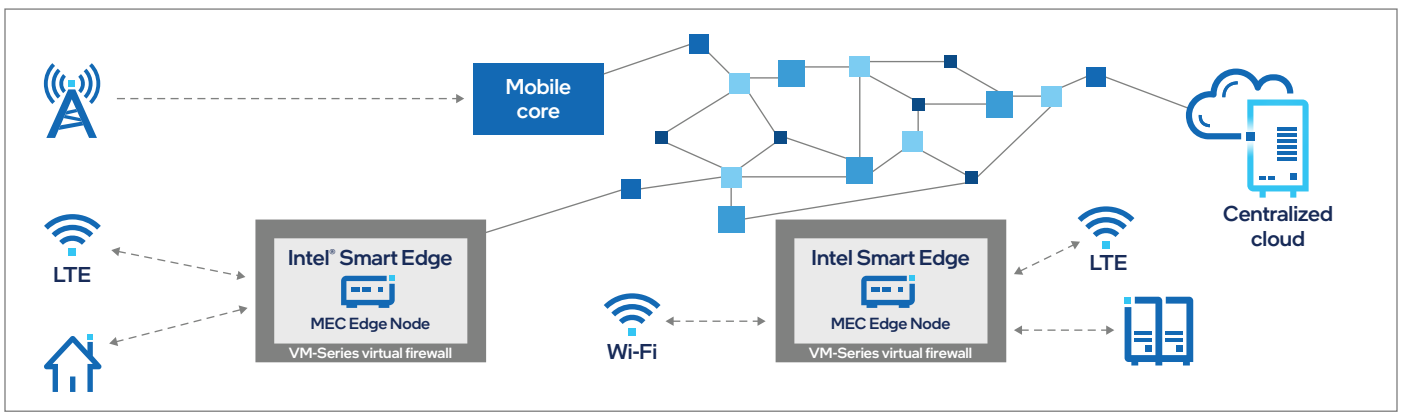
Networks are protected from threats that move within applications by providing multiple layers of protection. This strategy can identify and block threats on any network ports.

6. Global threats

A worldwide community of customers share global threat intelligence. This collaboration stops advanced attacks shortly after they are encountered. Global threat intelligence can significantly reduce the success rate of malicious attacks.

They can also achieve a higher return on investment by deploying Palo Alto Networks' VM-Series virtual firewall alongside Intel Smart Edge.

Intel® Smart Edge architecture plus Palo Alto Networks' VM-Series virtual firewall



Unique high-level benefits of a joint solution with Intel Smart Edge and Palo Alto Networks' VM-Series virtual firewall

The VM-Series virtual firewall is the world's first machine learning, next-generation intelligent firewall. It delivers powerful, automated features that minimize the risk of infection, maximize the user experience, and increase efficiency of IT operations.

In-line machine learning prevents up to 95 percent of new threats instantly and directly on the firewall.[1] Machine learning algorithms are embedded in the firewall code to minimize risk. The firewall can inspect a file while it's being downloaded and block malicious files without having to access online tools. The VM-Series virtual firewall monitors all traffic and behavior across IoT and connected devices, extending visibility and protection without the need for additional hardware.

The firewall uses zero-delay signatures for threats that can't be blocked in-line. These signatures are delivered continuously and in near-real time from the cloud for rapid prevention. If a threat is detected, the staff can identify it quickly. Administrators can save time and effort with automated intelligent policy recommendations, helping to eliminate human error and breaches caused by misconfiguration.

Palo Alto Networks' VM-Series machine learning–powered next-generation intelligent firewall increases the security and efficiency of IT operations. And along with the integrated security features of Intel Smart Edge, the solution creates highly effective MEC/edge cloud security.

Capacity on VM-Series virtual firewalls

Palo Alto Networks' virtual firewall is the first in the industry to move away from rigid models to cloud-like consumption. Software credits allow full flexibility in defining and allocating vCPU performance to all Palo Alto Networks software and firmware platforms.

Refer to Table 1 for VM-Series capacity details by memory allocation. For full capacity specifications, visit paloaltonetworks.com/products/product-selection.

Refer to Table 2 for VM-Series throughput figures. For full performance specifications and environment-specific data sheets, visit paloaltonetworks.com/products/product-selection.

Memory (min.)	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
Sessions	64,000	250,000	819,200	2,000,000	10,000,000
Security rules	250	1,500	10,000	10,000	20,000
Dynamic IP addresses	2,500	5,000	10,000	32,000	100,000
Security zones	15	40	40	200	200
IPsec VPN tunnels	250	1,000	2,000	4,000	8,000
SSL VPN tunnels	40	100	400	1,200	2,500

Table 1: VM-Series capacity details by memory allocation.

For full capacity specifications, visit paloaltonetworks.com/products/product-selection.

vCPU configuration	VM-Series 2 vCPU	VM-Series 4 vCPU	VM-Series 5 vCPU	VM-Series 8 vCPU	VM-Series 16 vCPU	VM-Series 22 vCPU
APP-ID throughput	3 Gbps	6 Gbps	6 Gbps	12 Gbps	19 Gbps	28 Gbps
Threat prevention throughput	1.5 Gbps	3 Gbps	4 Gbps	6 Gbps	13 Gbps	14 Gbps

Table 2: VM-Series throughput

Performance varies across different hypervisors and cloud environments. Refer to environment-specific data sheets for associated performance. For full performance specifications, visit paloaltonetworks.com/products/product-selection.

Conclusion

Organizations have a growing demand for cloud computing, 5G connectivity, and near-real-time dataflows and content. These demands have created a need for low-latency computing and security at the network edge. However, this need has presented many challenges as IT deploys MEC servers.

Intel Smart Edge helps minimize these challenges. It provides the low latency, simplicity, and open architecture that organizations need to roll out LTE, 5G, or Wi-Fi connectivity. This joint solution combines the Intel Smart Edge and Palo Alto Networks' VM-Series virtual firewall. Together, they can create a high level of security and efficiency for IT operations with MEC servers.

About Palo Alto Networks

Palo Alto Networks, a global cybersecurity leader, continually delivers innovation to enable secure digital transformation, even as the pace of change is accelerating. They provide visibility, trusted intelligence, automation, and flexibility to help complex organizations advance securely. Palo Alto has a comprehensive portfolio and growing ecosystem of partners. Together they protect tens of thousands of organizations across clouds, networks, and mobile devices.

paloaltonetworks.com

Learn more

Get more details about Palo Alto Networks' VM-Series virtual next-generation firewall.

Take an ultimate test drive ›

Download the VM-Series virtual firewall spec sheet ›

Visit the website ›

Learn more about the Intel® Smart Edge platform ›

intel + paloalto NETWORKS

1. Source: Palo Alto Networks internal testing data. https://www.paloaltonetworks.com/cyberpedia/what-is-an-ml-powered-ngfw