Palo Alto Networks and Corsa Security
Automated Scaling of VM-Series Firewall Clusters for Terabit Inspection

KEY DRIVERS
Organizations are looking to inspect large volumes of traffic while ensuring:

- **Business agility**
- **Ease of deployment and operations**
- **Risk mitigation**
- **Security robustness**

SOLUTION
Corsa Security Orchestrator scaling Palo Alto Networks VM-Series virtual firewall clusters

BENEFITS

- **Enjoy cloud-like elasticity and manageability of on-premises virtual network firewall clusters.**
- **Maintain predictable performance for any inspection and threat prevention based on intelligent software load balancing**
- **Eliminate inspection limitations with scale-out architecture that automates cluster upgrades.**
- **Speed deployment and time to service with automated virtualization workflows and deploy a consistent solution across all sites or zones to minimize training and support**
- **Use linear scaling for best entry level economics and leverage a pay-as-you-grow Corsa Security subscription model with Palo Alto Networks credit-based (Flex) licensing for 5x improved economics.**

USE CASES
- **Protect Private 5G network**
- **Protect MEC infrastructure**
- **Secure trust boundaries within the private network**
- **Secure the internet-edge**

About Corsa Security

Corsa Security is the leader in automating network security virtualization, which helps large enterprises and service providers deploy, scale and optimize virtual on-premise firewalls with speed (24x faster deployment), simplicity (zero-touch operations) and savings (9x lower TCO).

Visit **corsa.com**

The Challenge

Industry 4.0 is driving enterprises and service providers to embrace 5G for a hyper-connected and always on network that is quite different from their traditional wireless/wireline networks. New 5G architectures – such as private 5G networks, Multi-Access Edge Computing (MEC) and network slicing — give enterprises a new level of control but they must now deal with new and broader cybersecurity challenges.

Scaling network security has always been challenging in any network. But, in this new 5G world with vast numbers of IoT devices, there is a need to provide terabit-scale traffic inspection capacity that can be rapidly deployed and dynamically scaled without affecting the performance of these 5G networks.

The Solution

The Corsa Security approach to network firewall virtualization simplifies how large enterprises and service providers scale traffic inspection at much lower total cost of ownership (TCO). By tightly integrating virtualization with intelligent orchestration, Corsa Security streamlines deployment, scaling and optimization of virtualized next generation firewall (NGFW) clusters for large networks. Customers deploy virtual firewalls rapidly and with ease and then pay as they grow while never having to deal with infrastructure.

Key to this is the Corsa Security Orchestrator (CSO) which binds the worlds of network security (the firewall inspection) to the underlying network (server infrastructure). It performs key functions required for large-scale firewall virtualization and traffic inspection:

- Automation of bootstrap and initial configuration of NGFW VMs
- Provisioning of policy settings to the VMs in a zero-touch way
- Software load balancing for optimal virtual firewall performance within clusters
- Flow tracking for intelligent traffic steering to and from VMs
- Health check mechanism to monitor VM and system performance
- Push-button virtual firewall cluster upgrades to scale to Tbps

How it Works

The CSO lets users spin up and down virtualized inspection capacity by intelligently load balancing traffic between as many Palo Alto Networks VM-Series instances as needed. VM creation and performance is managed seamlessly from the CSO which is tightly integrated with Palo Alto Networks Panorama™ policy management, enabling chassis-scale stateful inspection to be performed using clusters of VM-Series instances within a customer's existing security stack.

This fully integrated solution is transforming traditional network security to software-defined network security, allowing users to have a cloud-like experience on-premise for managing their virtual network firewalls. With the click of a button, one can predictably add inspection capacity without worrying about network performance.

5G Private Network Use Case

Challenge

Having full visibility and network security for devices using industry 4.0 enabled applications through 5G is critical. Further, enterprises want full control over who and what gets sent to where in their geographically distributed networks. To protect their infrastructure and data from private 5G to the cloud and the edge deployment to the internal network, security must be granular yet able to quickly scale to very high levels.

Solution

To increase threat protection, virtual firewalls, like Palo Alto Networks VM-series inspect all the traffic flowing through the network and offer flexibility and agility. But to scale, you need to link the virtual firewalls together into clusters with a system that's easy-to-configure and monitor.

The Corsa Security solution can software load balance and orchestrate traffic across multiple VM-Series instances in a cluster to easily inspect all of your traffic. As traffic continues to grow, scaling inspection is as easy as a single-click in the Corsa Security Orchestrator to perform a cluster upgrade which adds more VM-Series resources.
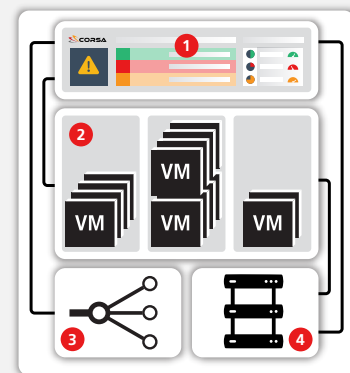
With Corsa Security and Palo Alto Networks, customers start to apply policy and inspect traffic within hours of delivery as the integrated offering can be deployed into any network without requiring changes in the network design.

Deployment

The whole system is extremely simple to deploy. Corsa Security provides the necessary orchestration software that creates and controls VMs running on your commodity servers installed in your private network. With the appropriate number of credit-based licenses for Palo Alto VM-Series instances, virtual firewalls are created and sized to meet the needs of your private 5G network.

The cloud-like design gives you the ultimate elasticity and manageability to provide each network zone with the specific amount of inspection required and then scale that inspection as needed, on a per zone basis. With virtualization, you do not need to bring in new hardware but simply add inspection virtually and remotely.

Plus, turning on CPU intensive inspection features are no longer a problem because the solution scales out horizontally, delivering predictable performance for all your network security needs. This eliminates the traditional trade-off between security coverage and network performance. If, at any time, you notice that performance is decreasing you can spin up additional virtual firewalls which are added to the cluster to increase inspection capacity.

1 Corsa Security Orchestrator
2 Palo Alto Networks VM-Series Virtual Firewalls
3 Corsa Security Software Load Balancer
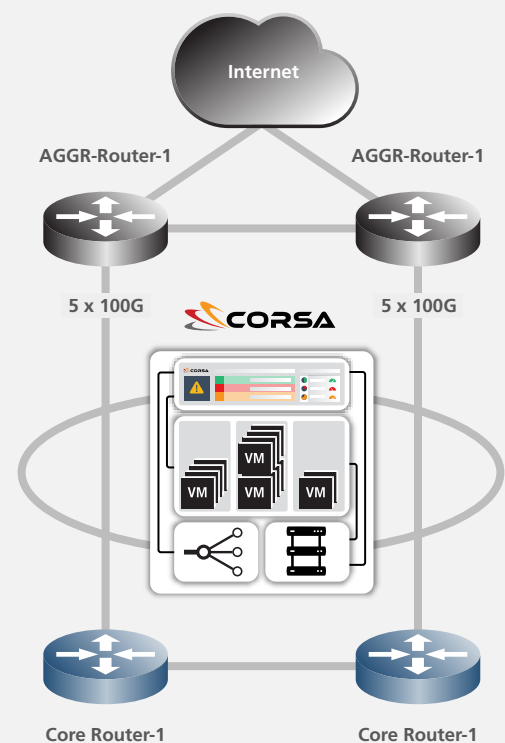**4** Commodity 'bring your own' Server

FIGURE 1: Turnkey Network Security Virtualization

FIGURE 2: 260G Site example