USE CASE

Complete Communications Monitoring with Push-Button Scaling of Traffic Inspection Capacity

National security agencies, large organizations, and law enforcement frequently conduct analysis of data communications. It's essential for national security, the investigation of serious crimes, as well as the investigation of threats to networks, individuals and organizations. To be effective in an increasingly digitized society, these organizations need full threat protection and want traffic monitoring with unlimited scale, so it can easily and quickly expand to meet increasing demands. Traffic monitoring needs to keep pace with current and future technologies, as well as offering agility and flexibility to fine-tune traffic monitoring and intercept very quickly when needed.

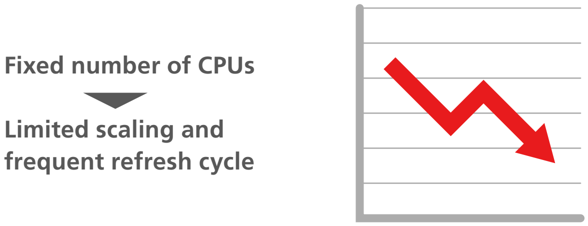


Figure 1: Using appliances means relying on a fixed number of CPUs that limits scale and requires frequent attention

Problem

INCREASES IN TRAFFIC VOLUME AND ENCRYPTION PREVENT EFFECTIVE MONITORING

With the exponential increase in traffic volume and a high percentage of that traffic encrypted (over 75%), agencies and other large organizations need to inspect an ever-expanding volume of encrypted network traffic. Additionally, criminal and terrorist organizations regularly communicate, organize and fundraise using encrypted communications.

Currently, this traffic monitoring is hardwired into the network path so if an organization has 40Gbps of connectivity, they need 40Gbps worth of inspection capability. Since security appliances are hardware-based with a fixed capacity limit, any change to increase traffic monitoring means undertaking a network change. The additional firewalls can only inspect so much traffic before the cycle repeats due to ever growing traffic volumes.

The risk of unchecked traffic

As well as being time-consuming and expensive, this leaves the organization in a reactive position. What's more, even the largest firewalls suffer performance degradation when trying to use next-generation features such as URL filtering or SSL inspection. Throughput can suffer by up to 90% when these features are turned on. Organizations can't accept this impact to their network's performance, so they opt to let traffic through unmonitored in order to speed up their network.

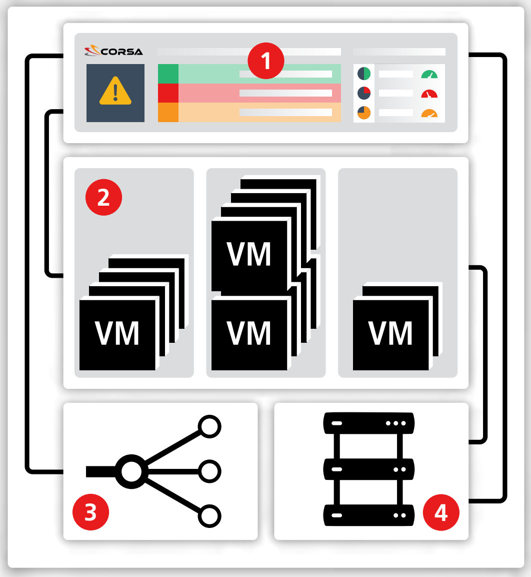
This approach to Communications Monitoring is failing us:

- Increasing monitoring requirements decreases network throughput.
- It's impossible to predict traffic growth, meaning organizations over provision.
- Scaling inspection and threat protection always reaches a finite limit.
- Different needs for different sites means different hardware, which complicates operations.

Solution

SCALE INSPECTION WITHOUT KILLING NETWORK PERFORMANCE

The turnkey Corsa Network Security Virtualization Platform scales traffic inspection and threat protection without impacting network performance. By integrating firewall virtualization with intelligent orchestration, it streamlines deployment, management and operations of virtualized next-generation firewall (NGFW) arrays for large networks.



1. **Corsa Security Orchestrator**
2. **Virtualized firewall**
3. **Corsa Security Services Load Balancer**
4. **Commodity compute servers**

Figure 2: Turnkey Network Security Virtualization delivered as a fully integrated platform

You get push-button scaling of communications monitoring by distributing traffic inspection across as many virtual firewall instances as the needs dictate. Behind the scenes, the virtual NGFWs are running on state-of-the-art hyperconverged infrastructure, specifically optimized for scaling network security.

Intelligent Orchestration

A key element of the integrated solution is the Corsa Security Orchestrator which binds the worlds of network security (the firewall) together with the network. It performs key functions required for large-scale firewall virtualization:

- Automation of bootstrap and initial configuration of NGFW VMs
- Provisioning of policy settings to the VMs in a zero-touch way
- Stateful connection tracking for intelligent traffic steering to and from VMs
- Health check mechanism to monitor VM and system performance

This lets you elastically add virtualized NGFW L7 inspection capacity to meet the demands for increasing inspection and traffic monitoring with the click of a button.

Deployment

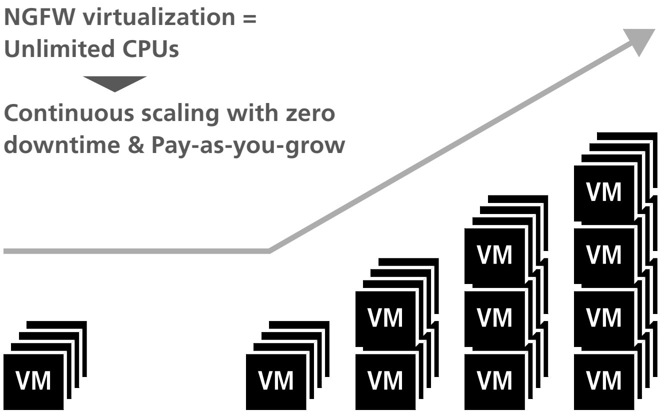
MANAGE AND SCALE YOUR INSPECTION FROM A CENTRAL LOCATION

The Corsa Security solution offers rapid deployment which is critical for organizations addressing ever increasing traffic volumes. You can scale your traffic inspection quickly and easily across multiple sites, all from a single dashboard.

It's a single solution that is deployed at separate sites with variable traffic bandwidth, inspection capacity, as well as configuration and connection requirements. The solution scales traffic inspection quickly and easily - from 10 Gbps to many 100 Gbps of inspection - from one centralized location. This means you no longer need on-site intervention to respond in real-time to monitoring needs. It can be adapted across all the deployments to maximize operational efficiencies.

Virtual Management

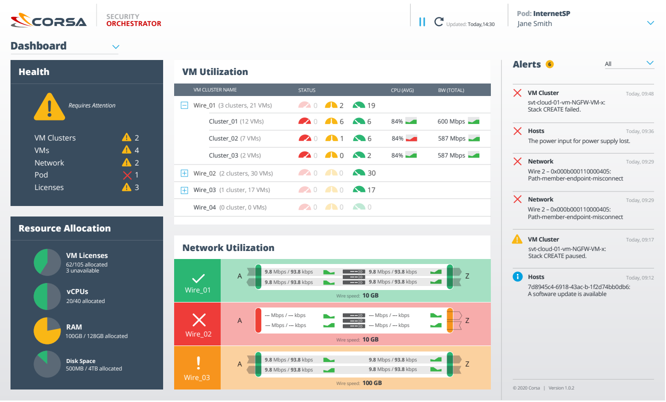
Leveraging a single pool of firewall virtual machines (VMs), you can shuffle VM licenses between sites to allocate inspection where it's most needed. The network team determines and can dynamically change what security policy profile to use at each site. When additional traffic monitoring is required, the team can add virtual firewalls at the appropriate site.



NGFW virtualization = Unlimited CPUs

Continuous scaling with zero downtime & Pay-as-you-grow

Figure 3: Turnkey network security virtualization scales inspection for communications monitorings



CORSA | SECURITY ORCHESTRATOR

Updated: Today,14:30

Pod: **InternetSP**
Jane Smith

Dashboard

Health

Requires Attention

VM Clusters	⚠ 2
VMs	⚠ 4
Network	⚠ 2
Pod	✕ 1
Licenses	⚠ 3

Resource Allocation

VM Licenses 62/105 allocated 3 unavailable

vCPUs 20/40 allocated

RAM 100GB / 128GB allocated

Disk Space 500MB / 4TB allocated

VM Utilization

VM CLUSTER NAME	STATUS			CPU (AVG)	BW (TOTAL)
Wire_01 (3 clusters, 21 VMs)	0	2	19		
Cluster_01 (12 VMs)	0	6	6	84%	600 Mbps
Cluster_02 (7 VMs)	0	1	6	84%	587 Mbps
Cluster_03 (2 VMs)	0	0	2	84%	587 Mbps
Wire_02 (2 clusters, 30 VMs)	0	0	30		
Wire_03 (1 cluster, 17 VMs)	0	0	17		
Wire_04 (0 cluster, 0 VMs)	0	0	0		

Network Utilization

✓ Wire_01
A
9.8 Mbps / 93.8 kbps | 9.8 Mbps / 93.8 kbps
9.8 Mbps / 93.8 kbps | 9.8 Mbps / 93.8 kbps
Z
Wire speed: **10 GB**

✕ Wire_02
A
--- Mbps / --- kbps | --- Mbps / --- kbps
--- Mbps / --- kbps | --- Mbps / --- kbps
Z
Wire speed: **10 GB**

! Wire_03
A
9.8 Mbps / 93.8 kbps | 9.8 Mbps / 93.8 kbps
9.8 Mbps / 93.8 kbps | 9.8 Mbps / 93.8 kbps
Z
Wire speed: **100 GB**

Alerts 6 All

✕ **VM Cluster** Today, 09:48
svt-cloud-01-vm-NGFW-VM-x:
Stack CREATE failed.

✕ **Hosts** Today, 09:36
The power input for power supply lost.

✕ **Network** Today, 09:29
Wire 2 – 0x000b000110000405:
Path-member-endpoint-misconnect

✕ **Network** Today, 09:29
Wire 2 – 0x000b000110000405:
Path-member-endpoint-misconnect

⚠ **VM Cluster** Today, 09:17
svt-cloud-01-vm-NGFW-VM-x:
Stack CREATE paused.

ℹ **Hosts** Today, 09:12
7d8945c4-6918-43ac-b-1f2d74bb0db6:
A software update is available

© 2020 Corsa | Version 1.0.2

Single Dashboard

The Corsa Security Orchestrator is integrated with the firewall policy manager to provide a single pane of glass for monitoring and policy management. The inspection requirements for all sites are addressed and managed through a single dashboard with each Corsa Security platform tuned for site-specific capacity and policy. Therefore, the network team only has to manage a single firewall configuration, instead of having to source different size firewalls.

A Modern Approach using Virtualization

Digital transformation is a strategic imperative, especially for mission-critical functions like national communications monitoring and enterprise threat protection. This solution fits within your existing network with the least disruption, leverages virtualization so it's dynamic, allowing you to modernize your interception system but maintain consistency with current technologies. It also means minimal new skills training.

Benefits

ADAPTABLE COMMUNICATIONS MONITORING FOR MULTIPLE SITES

When organizations need adaptable communications monitoring but can't keep up with inspecting the high volume of incoming traffic *and* maintaining their network's performance, they need a robust solution which dynamically scales traffic inspection at the touch of a button.

Complete visibility

You get full visibility by inspecting 100% of the traffic you need to. Regardless of differences in traffic volume, mix, encryption levels, or site locations, you can fully monitor all the communications of interest at all times.

Dynamic scaling

With no hardware to purchase, install, test or maintain, you can spin up your inspection capacity at the touch of a button. This allows for site variations and the option to broaden your monitoring capabilities in the future.

Intuitive virtualization

Built with a simple and intuitive UI, the Corsa Security Orchestrator is a single portal to set up and orchestrate all virtual NGFWs. You manage inspection for all of your sites from a central control.

Consistent experience

Consistent deployment across multiple sites and unified, centralized control means reliable communications monitoring, as well as minimal training and support.

Pay-as-you-Grow

You gain a huge reduction in TCO by virtualizing hardware. You make a precise investment by purchasing exactly what you need (pay-as-you-grow) and benefit from predictable costs by moving to an OPEX model.

The Corsa Security solution can be quickly deployed by national security agencies, law enforcement, and large organizations to effectively monitor electronic communication. It can scale traffic inspection across multiple sites, all from a single dashboard, which is critical for organizations addressing ever increasing traffic volumes.

About Corsa Security

Corsa Security is the leader in scaling network security with the first turnkey network security virtualization platform that simplifies how large enterprises and service providers scale traffic inspection, including SSL/TLS encrypted, at much lower total cost of ownership (TCO). By tightly integrating virtualization with intelligent orchestration, Corsa Security streamlines deployment, management and operations of virtualized next generation firewall (NGFW) arrays for large networks. Customers subscribe to the Corsa Security service based on their traffic inspection capacity needs and then pay as they grow while never having to deal with the infrastructure. Learn how Corsa is revolutionizing network security at **corsa.com**.