CORSA

USE CASE

Close the SSL Inspection Gap with Turnkey Virtualization for 100% Visibility

Organizations are increasing their reliance on encryption, primarily secure sockets layer (SSL) and transport layer security (TLS), to protect their data in motion. At the same time, cybercriminals are using encrypted traffic to obscure their presence and evade detection while going about their nefarious business.

The bad news for high capacity links is that few security devices can keep up with this amount of encrypted traffic, meaning cybercriminals have an open door. To secure their networks, organizations need a solution which can scale SSL/TLS visibility in an economical way in order to inspect all traffic passing through their network.

The performance impact for traffic inspection is

60%

on average

A firewall device of ~35Gbps of throughput can only deliver

5.8 Gbps

of SSL/TLS inspection

Up to

92%

throughput drop when SSL/TLS inspection is enabled

Decreased SSL/TLS inspection capability

Problem

ENTERPRISES CAN'T KEEP UP WITH DECRYPTING INCOMING TRAFFIC

With the exponential increase in traffic volumes and mix along with over 70% being encrypted, enterprises face ever-expanding vulnerabilities when it comes to cybersecurity because of the SSL Inspection Gap.

The SSL Inspection Gap is the point where an enterprise can't keep up with decrypting incoming traffic and maintain their network's performance, so they opt to turn off SSL/TLS decryption on their firewalls and let traffic through unchecked in order to speed up their network.

Throughput drops up to 92% when SSL/TLS inspection is enabled

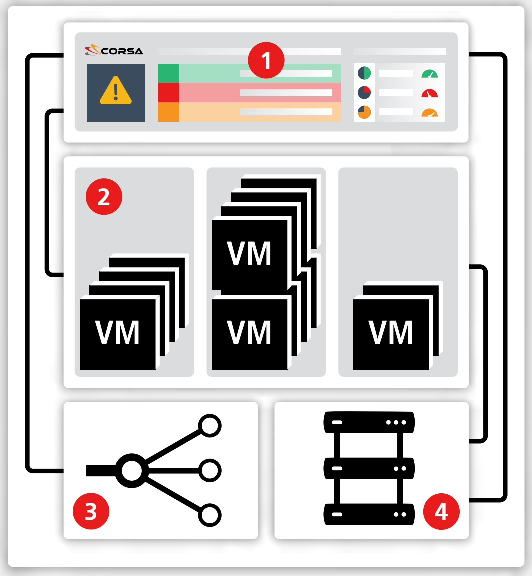
NSS Labs runs detailed testing of security devices to measure both their ability to inspect encrypted traffic and the impact of this on forwarding performance. It is not pretty. On average, the performance impact for traffic inspection is 60 percent and throughput drops by up to 92 percent when SSL/TLS inspection is enabled. Tests and supporting literature confirm that a firewall device of ~35Gbps of throughput can only deliver 5.8 Gbps of SSL/TLS inspection.

Since firewall performance is hardwired into your network path, you have to carefully plan for enough inspection capacity to prevent this SSL Inspection Gap. For example, if you have 40Gbps of connectivity, you need 40Gbps worth of encryption/decryption capability (or at least a reasonable amount that is closer to your traffic profile). The real challenge is, every time you upgrade your connectivity or the traffic increases beyond your current capacity, you have to bring in a bigger box. The cost, time and labor investment this demands makes it unsustainable; you will never keep up with your capacity requirements if you follow this approach.

Solution

A TURNKEY NETWORK SECURITY VIRTUALIZATION PLATFORM PROVIDES 100% SSL/TLS VISIBILITY

To achieve complete 100% SSL/TLS visibility while guaranteeing network performance, you need to virtualize your network security. This allows you to spread encryption/decryption functions within your virtual next generation firewalls (NGFW) across several virtual machines (VMs) so that you're no longer tied to the performance of a single firewall appliance and you can scale out security inspection horizontally.



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

Figure 1: Turnkey network security virtualization platform

Virtualization is not trivial

That said, actually implementing network security virtualization is far from trivial. To successfully implement large-scale virtual firewalls, you need to be able to easily spin up whatever inspection capacity you require from a dashboard where you also orchestrate and manage all your VMs, within the context of your network. That's a lot to achieve, including:

- determine the right commodity server for the NGFW VMs to run on
- install hypervisor software on the server
- bootstrap, upgrade the software, and configure the NGFW VMS
- scale one NGFW virtual instance to many
- create virtual NGFW arrays of any inspection capacity.

What's more, to perform SSL decryption, both directions of any connection always need to pass through the same decryption processing node even as VMs are added or removed. To do this, you need load balancing technology with automatic path checks and member synchronization, including automatic re-balancing if a VM failure is detected.

So, it must be turnkey

It's a very complex system and requires expertise from networking to firewalling to security. Or, if it's bundled together as a platform and offered up as turnkey, you can provision your SSL/TLS inspection capacity with a simple click of a button, and add as much inspection capacity as you require to meet traffic demands predictably.

The turnkey Corsa Network Security Virtualization Platform does just that and solves the SSL Inspection Gap by providing 100% visibility without degrading performance. By tightly integrating virtualization with intelligent orchestration, Corsa Security streamlines deployment, management and operations of virtualized NGFW arrays for large networks.

Deployment

SETUP IN MINUTES AND SCALE TRAFFIC INSPECTION WITH THE CLICK OF A BUTTON

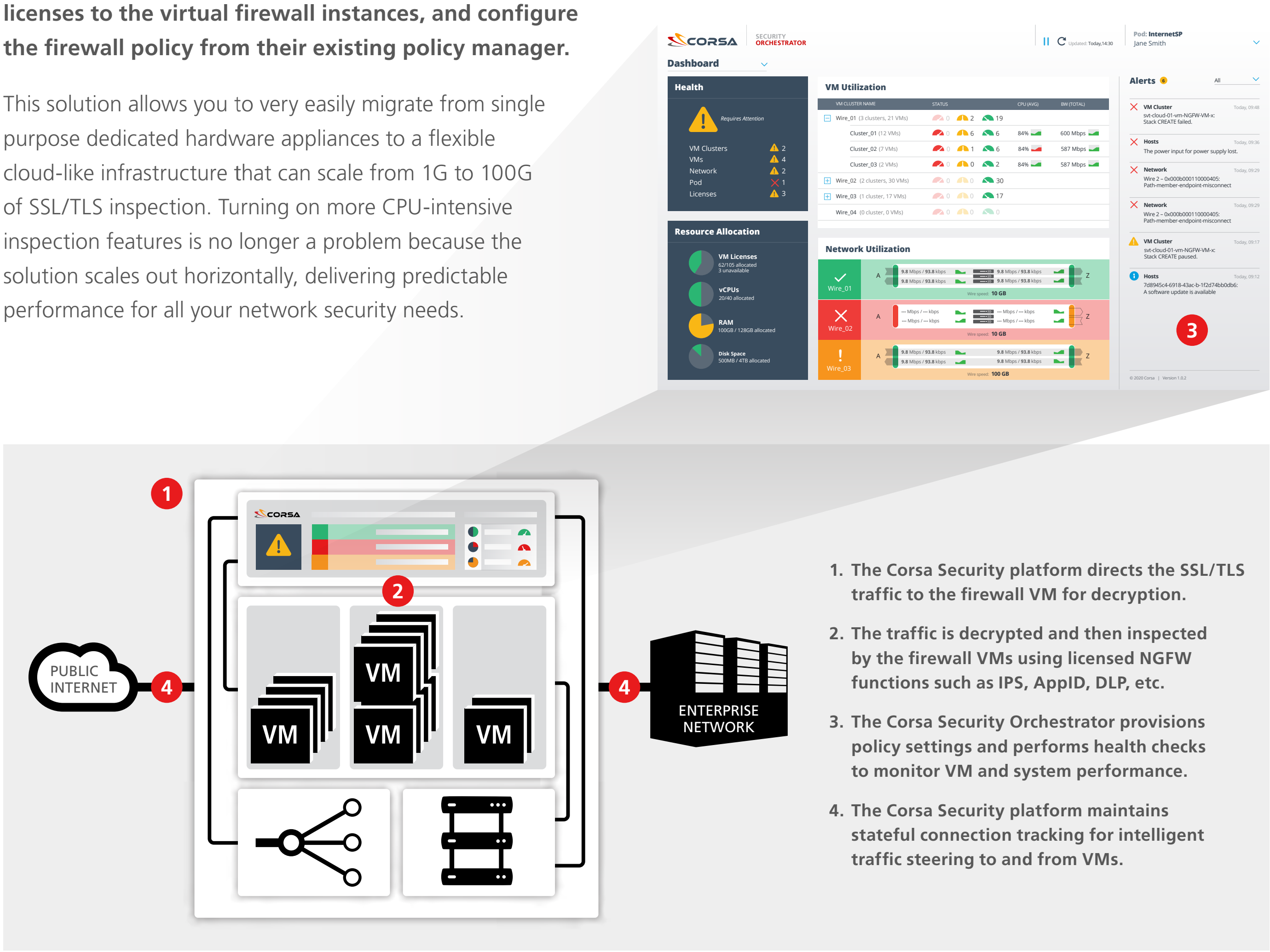
The Corsa Security platform is extremely simple to use. From the network perspective it is deployed as a virtual wire firewall on any high capacity link. Corsa Security provides all the necessary network, server, load balancing and management components in a turnkey HCI package. You continue to use your preferred security vendors, while behind the scenes their virtual functions are running on state-of-the-art hyperconverged infrastructure, specifically optimized for scaling SSL/TLS inspection. You just need to provide the appropriate licenses to the virtual firewall instances, and configure the firewall policy from their existing policy manager.

This solution allows you to very easily migrate from single purpose dedicated hardware appliances to a flexible cloud-like infrastructure that can scale from 1G to 100G of SSL/TLS inspection. Turning on more CPU-intensive inspection features is no longer a problem because the solution scales out horizontally, delivering predictable performance for all your network security needs.

Managed through a single dashboard

Different inspection requirements across different sites can be addressed and managed through a single dashboard that is tightly integrated with the firewall policy manager, so each Corsa Security platform can be tuned for site-specific SSL/TLS inspection capacity. Therefore, the network team only has to manage a single configuration, instead of having to source different size firewalls or SSL/TLS inspection appliances.

Leveraging a single pool of firewall VMs, you can shuffle VM licenses between sites to allocate inspection where it's most needed. This means you only deploy the exact SSL/TLS inspection capacity you need at any given time.



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

VM Licenses 62/105 allocated 3 unavailable
vCPUs 20/40 allocated
RAM 100GB / 128GB allocated
Disk Space 500MB / 4TB allocated

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		

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.

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

© 2020 Corsa | Version 1.0.2

1. **The Corsa Security platform directs the SSL/TLS traffic to the firewall VM for decryption.**
2. **The traffic is decrypted and then inspected by the firewall VMs using licensed NGFW functions such as IPS, AppID, DLP, etc.**
3. **The Corsa Security Orchestrator provisions policy settings and performs health checks to monitor VM and system performance.**
4. **The Corsa Security platform maintains stateful connection tracking for intelligent traffic steering to and from VMs.**

Figure 2: Deploy seamlessly into existing architecture and manage through a single-pain-of-glass

Benefits

SCALE YOUR RAPIDLY CHANGING INSPECTION REQUIREMENTS QUICKLY, EASILY AND AFFORDABLY

When you scale SSL/TLS inspection using the turnkey Corsa Security platform, you can be sure that you are seeing all the traffic entering your network. The result is complete SSL/TLS visibility with so much more:

Increased agility

With your SSL/TLS inspection virtualized, there is no security hardware to purchase, install, test, or maintain. You dramatically reduce the time you need to turn on more inspection capacity.

Stronger security

You can enable all the SSL/TLS inspection you need at no performance penalty to the network. This eliminates the traditional trade-off between security and network performance, which prevents malicious traffic entering the network uninspected.

Lower TCO

You pay-as-you-grow for only the inspection capacity you need. You don’t need to worry about over-provisioning your firewall capacity, giving you at least 2x lower TCO than current solutions.

Improved IT operational efficiency

Built with a simple and intuitive UI, the Corsa Security Orchestrator is a single portal to set up and orchestrate all virtual NGFWs. You also use your existing firewall policy manager, which eliminates the need for additional training.

Future proofing of security

As your needs grow and change, you can evolve, update, or expand the virtual security functions you use. This gives you long-term consistency in your traffic inspection with future flexibility to manage your growing network.

Solving the SSL Inspection Gap is critical for enterprises to gain 100% visibility and prevent cyberattacks. With turnkey network security virtualization you can stay on top of your rapidly changing capacity requirements quickly, easily and affordably.

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**.