CORSA

USE CASE

Increase Threat Protection by Using All Your NGFW Features Without Impacting Performance

In today's perfect storm, security and network architects have to choose between full threat protection or optimal network performance. Independent studies confirm there is up to a 90% drop in firewall performance when SSL/TLS decryption is enabled. The problem is, if you turn SSL/TLS decryption off then many of the NGFW features don't work on the 75+% of traffic which is encrypted. But, if you turn on those NGFW features, your network performance drops even more. It's a lose-lose situation.

Security and network architects find themselves asking, "Which NGFW features will I be able to use before I kill the network?" These features aren't just nice-to-have; they're essential to threat protection. They need a way to use these features while keeping their networks running.

Up to

90%

drop in performance when SSL/TLS decryption is enabled

75%

of today's Internet traffic is encrypted

Problem

TURNING ON ALL YOUR NGFW FEATURES KILLS YOUR NETWORK PERFORMANCE

Next generation firewalls (NGFW) are extremely feature rich. They do everything from VPN tunnel termination to intrusion prevention and application identification to content filtering, to name just a few.

These are extremely complex functions and require a huge amount of processing power. They also require traffic to be SSL/TLS decrypted/encrypted which comes with its own need for large amounts of CPU cycles. Combined, this results in poor performance of your single-purpose hardware security appliance.

That's why network and security teams spend countless hours tuning their appliances to find some balance between inspection capacity and network performance.

Despite their best efforts, there is always the risk of something unpredictable happening, like a new traffic pattern or a dynamic signature update, either of which would severely degrade the security device performance and more worryingly, open the network up to a new attack.

Let's take one example: **AntiVirus**. These days, this is a foundational security policy for many enterprises so they can see and manage attacks quickly, before they do irreparable damage. As well as scanning the system for spyware, adware, worms and other threats, anti-malware programs include advanced security features like behaviour monitoring, sandboxing and malware removal. All of these features are CPU intensive and need the traffic to be decrypted so you can see attacks in encrypted traffic.

As a result, AntiVirus is often left 'off' to maintain network performance. The root cause of the problem is the pure scale of traffic inspection required. And this is further exacerbated by the fact that more and more traffic entering a network from the Internet is SSL/TLS encrypted. There is no single CPU complex in the world that can stand up to this perfect storm. Third-party testing shows that single-purpose firewalls suffer up to a 90% drop in performance when SSL/TLS decryption is enabled but over 75% of today's Internet traffic is encrypted.

Solution

TURNKEY VIRTUALIZATION TO SCALE THREAT PROTECTION

There is another way. Turnkey virtualization using virtual firewalls makes it possible for you to dramatically increase your threat protection by benefiting from the full gamut of next generation firewall functions, including SSL/TLS decryption.

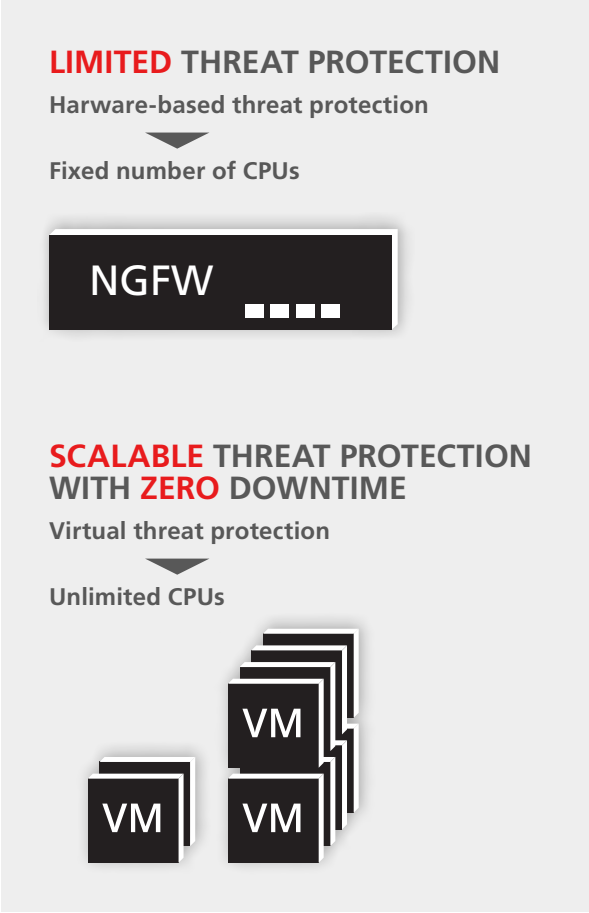

Figure 1: By virtualizing your threat protection capabilities you can distribute the work across unlimited CPUs.

Distributing the load

When you use a turnkey network security virtualization platform with in-line horizontal scaling, you decouple security from the network and eliminate the inverse relationship between security and network performance. This means you can use all your NGFW security profiles without impacting network throughput. All the features, all the time, to build the strongest defense possible.

Keep adding more CPUs

The security processing is done by many CPUs running separate virtual firewalls that each take care of a portion of your traffic inspection. These are the same virtual firewalls that public and private clouds leverage, pulled together into arrays of virtual machines that build up inspection capacity to meet north-south (N-S) traffic needs. So, features like AntiVirus can run freely regardless of how much traffic is encrypted. And, you can just add more CPUs with additional virtual firewalls when you need more inspection capacity. Network owners can fully benefit from the richness of this feature without impacting network performance.

Managed through a 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 requirements for all sites are addressed and managed through a single dashboard with each Corsa Security platform tuned for site-specific capacity and policy. You can shuffle VM licenses between sites to allocate capabilities where it's most needed. This means you only deploy the exact threat protection features you need at any given time.

Deployment

ADD CAPACITY AS NEEDED TO USE YOUR NGFW FEATURES

With the turnkey Corsa Security Platform, all the components run on an underlying hyper-converged infrastructure, which is deployed as a virtual wire firewall on any high capacity link.

This means users don't have to worry about hardware, servers, capacity, or specifying how much of one security appliance over another is needed and what the impact on the network will be.

Scale at the touch of a button

The architecture is scalable and flexible, so traffic inspection and threat protection capacity can be added or removed without any changes to the network or degradation of performance. Instead, virtual firewall instances are spun up and down with the click of a mouse to process your request.

NGFW FEATURES YOU CAN NOW TURN ON:

- AntiVirus
- Application Identification
- SSL/TLS Inspection
- Web Filter
- IPS
- DNS Filter
- Content Filtering
- And More

Let's return to the example of AntiVirus. When enabled, it keeps your network protected by preventing hackers from installing malicious software on PCs that can then be used to launch a variety of attacks from distributed denial of service (DDoS) to identity theft. These are features you don't want to lose for the sake of network performance, and the Corsa Security Platform allows you to scale them as needed without impacting the network.

FIREWALLS GO DIM WHEN NGFW INSPECTION GOES ON

Specification	Hardware-based Firewall Alone
Firewall throughput	200 Gbps
NGFW throughput	40 Gbps
SSL Inspection	35 Gbps
Threat	30 Gbps

- Application Identification
- IPS
- SSL/TLS Inspection
- AntiVirus
- Web Filter
- DNS Filter

INSPECTION GAP SOLVED

Specification	Hardware-based Firewall Alone	**Plus** Corsa Security Platform
Firewall throughput	200 Gbps	
NGFW throughput		Unlimited
SSL Inspection		Unlimited
Threat		Unlimited

- Application Identification
- IPS
- SSL/TLS Inspection
- AntiVirus
- Web Filter
- DNS Filter

Figure 2: A turnkey virtualization platform allows you to enable all the security policies without impacting performance.

Benefits

INCREASED THREAT PROTECTION

Now you can fully decrypt and inspect traffic without the concern of slowing down the network, and you can perform a variety of security functions on your wish list from App ID to AntiVirus and so much more.

The Full Suite of NGFW Features

Not only can you enable all the NGFW features and inspection capacity you need to prevent cyberattacks, the virtual wire deployment doesn't have an IP or MAC address so there is no added threat surface.

Predictable Performance

Thanks to dynamic scaling and intelligent load balancing, you gain network performance that is super steady and predictable, even when security posture increases.

Flexible Architecture

A network architecture with the flexibility to scale capacity and add security features dynamically. With no hardware to purchase, install or maintain, you can spin up your inspection capacity at the touch of a button.

Simplified Management

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, you can evolve, update, or expand the virtual security functions you use, as well as the NGFW features. This gives you long-term consistency in your traffic inspection with maximized threat protection whatever your future needs.

A turnkey network security virtualization platform can scale the processor-intensive network traffic inspection across many virtual firewall instances to effectively protect your network from security threats. Whether you have a single virtual firewall running or a large array of virtual firewalls to create gigabits of inspection, the performance of the network remains rock solid while the firewall inspection scales with all NGFW features enabled. You inspect 100% of the traffic you need to with an impressive amount of traffic inspection that dramatically reduces your risk of damage from a network attack at a significantly lower TCO. Build the best defense possible, save money, keep your peace of mind (and your job)!

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**.