SOLUTION BRIEF

Fortinet and Corsa Security Solutions

Leveraging the Power of Virtual Services to Scale SSL Decryption and Inspection

Executive Summary

The increased load of encrypted traffic is bogging down traditional hardware-based appliances. Today, more than 70% of all traffic in the network is being encrypted—a number that is rapidly on the rise.[1] Enabling inspection of encrypted traffic on hardware-based appliances can lead to a significant drop in performance, and these devices already struggle to keep up with high-performance demands from end-users.

Network administrators can find themselves turning off secure sockets layer (SSL) decryption and inspection in order to satisfy the demand for throughput, especially on high-volume north-south traffic links. However, this puts the network at risk to malware and other threats that may be carried over encrypted connections. Fortinet uses a more optimal hardware architecture by leveraging dedicated, customized security processors that offload CPU-intensive SSL overhead. As a result, organizations do not have to choose performance over security.

Fortinet and Corsa Security have partnered to deliver a solution that uses Corsa to virtualize and scale out FortiGate next-generation firewalls (NGFWs) to provide inspection capacity on-demand, as needed. FortiGate VM creation and performance is managed seamlessly from the Corsa Security Orchestrator, a virtualized infrastructure manager. Traffic is load balanced between FortiGate VM appliances that decrypt and inspect the traffic as needed. Sharing the load across as many virtual appliances as needed means there is no degradation of network performance or compromising security posture.

Fortinet and Corsa Joint Solution Description

Corsa delivers a turnkey network security virtualization platform that enables network owners to scale out their network security inspection with a single click. With the virtualized infrastructure manager, customers can easily increase their virtualized inspection capacity by adding as many FortiGate VM virtual appliances as needed. Corsa intelligently load balances traffic between all active FortiGate VM virtual appliances.

Gone are the days of firewall bottlenecks that cannot keep up with network traffic. The Corsa platform allows customers to apply any security policy without degrading network performance. Turning on CPU-intensive inspection features is no longer a problem because the solution scales out horizontally, delivering predictable performance to meet any network security need. As the load of encrypted traffic rises, more virtual appliances are easily added to the solution, sharing the inspection load.

Installed in virtual wire mode, the solution can be deployed into any network without requiring changes to the network architecture. The solution is easy to use and customers can start to apply policy and inspect traffic within hours of delivery.

Joint Solution Integrations

This joint turnkey platform transforms traditional network security to a software-defined networking security approach and delivers a cloud-like management experience for on-premises network security infrastructure. With a simple click of a button, customers can add inspection functions without fear of hindering performance. This scale-out approach helps inspect transport layer security (TLS) encrypted traffic at scale.

Joint Solution Benefits

Together, Fortinet and Corsa Security provide an integrated security solution for high-capacity networks that delivers:

- Cloud-like elasticity and manageability of on-premises network security and virtual appliances
- Predictable performance for inspection and threat prevention based on scale-out architecture
- Ability to eliminate dedicated hardware appliances and associated refresh cycles
- Support for multiple network security services simultaneously in the same platform
- Virtualized instances that allow customers to scale out inspection requirements as needed

FORTINET Fabric-Ready

The Fortinet and Corsa solution provides unparalleled levels of flexibility. Virtualized network security solutions make transitioning network security services as simple as shutting down old virtual appliances, and starting new ones. The same applies to NGFW software upgrades.

Virtual appliances run on state-of-the-art hyper-converged infrastructure (HCI) specifically optimized for in-line network security applications. The joint Fortinet and Corsa solution integrates five main elements:

Diagram of Joint Solution

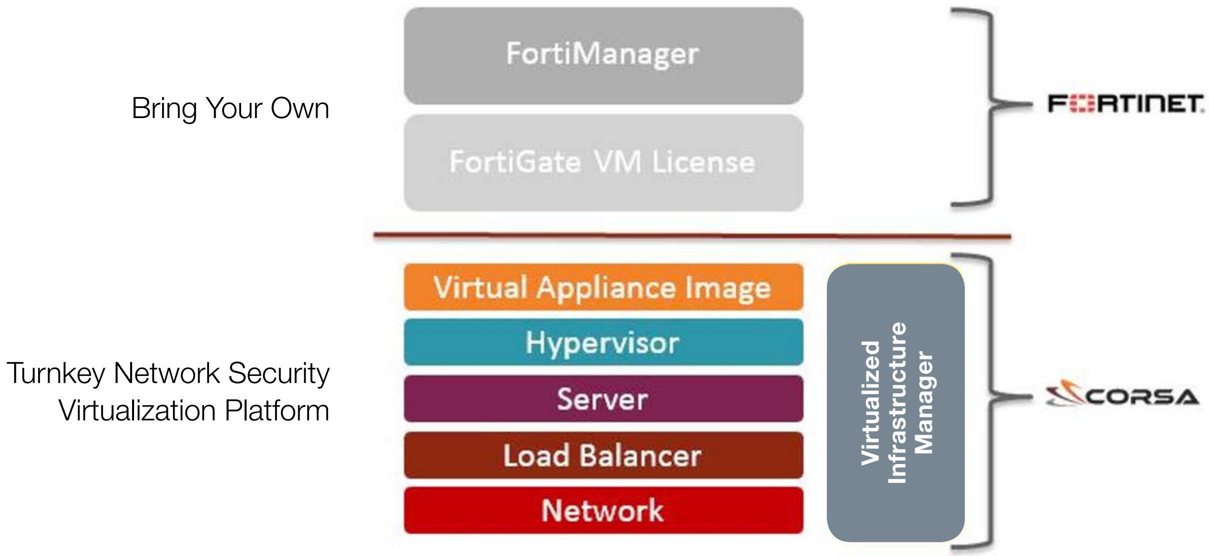

Figure 1: The Fortinet and Corsa Security joint solution stack.

Corsa Security Orchestrator. This virtualized infrastructure manager provides a cloud-like user experience for managing a virtualized network security infrastructure. It provides a simple way to provision and manage FortiGate VM appliances and the associated server, network, and load-balancing functions. It pushes the necessary initial configuration to the virtual appliances and allows them to be seamlessly integrated into FortiManager.

FortiGate VM NGFW. FortiGate-VM NGFWs perform in-depth network inspection and threat prevention, providing customers with the peace of mind that they maintain a strong security posture.

Security services load balancer. A virtual wire load balancer distributes the traffic to all virtual appliances and guarantees that both sides of any encrypted network connection are always sent to the same virtual appliance. This enables any stateful inspection to be performed on that connection, including TLS decryption. The load balancer also has built-in path check mechanisms that provide additional resilience and high availability.

Commodity compute servers with virtualization. Corsa Security technology is specifically optimized for in-line network security applications. These are based on Linux with a Kernel-based Virtual Machine (KVM) hypervisor and Single Root I/O Virtualization (SR-IOV) technology for networking to ensure the best possible performance for network security applications.

FortiManager. This centralized security management tool simplifies network orchestration, automation, and response. FortiGate-VM virtual appliances receive configuration and security policies from FortiManager, ensuring a consistent security policy is applied to the entire network. FortiManager offers single-pane-of-glass management and visibility and is part of a rich set of tools capable of managing more than 100,000 devices from a single console.

Corsa Virtualization

Corsa delivers a turnkey network security virtualization platform that scales out virtualized security appliances. It is a private cloud approach to scale traffic inspection so customers can elastically add capacity to meet increasing bandwidth demands. Network owners no longer need to deal with hardware and can focus on security policies while Corsa take scales traffic inspection and other network security services. The Corsa Security Orchestrator makes controlling and monitoring of the system simple.

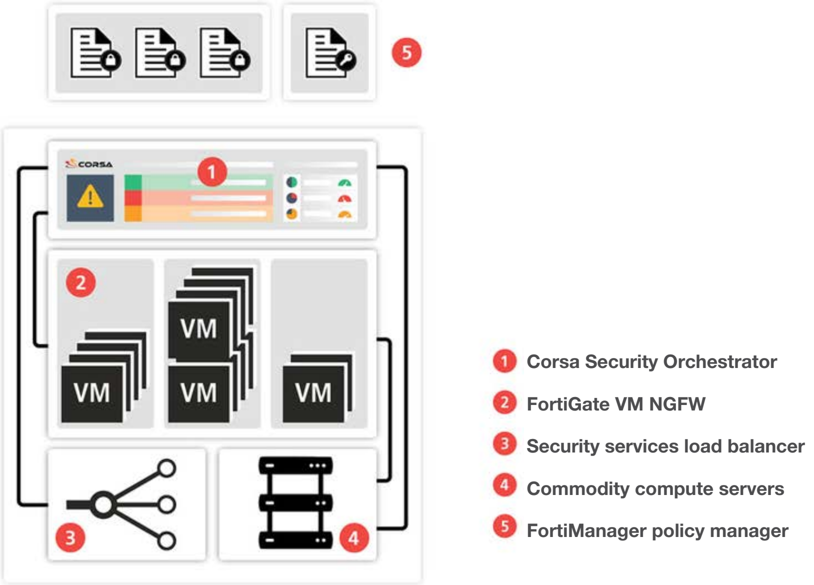
5
CORSA
1
2
VM
VM
VM
VM
3
4
1 Corsa Security Orchestrator
2 FortiGate VM NGFW
3 Security services load balancer
4 Commodity compute servers
5 FortiManager policy manager

Figure 2: Virtual wire deployment of Corsa Security and FortiGate VM firewall.

Fortinet FortiGate NGFW and FortiManager

The Fortinet FortiGate NGFW combined with FortiManager deliver top-rated protection and high performance. FortiGate reduces infrastructure complexity with automated visibility into applications, users, and the network, and provides security ratings to adopt security best practices. The FortiGate VM NGFW is scalable and capable of dealing with high levels of encrypted traffic without a performance degradation.

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 streamlines deployment, management, and operations of virtualized NGFWs for large networks.

Learn more at: www.corsa.com.

[1] John Maddison, "Encrypted Traffic Reaches A New Threshold," Network Computing, November 28, 2018.