CORSA

USE CASE

Offer a Managed Network Firewall Service in Minutes with the Click of a Mouse

Cyberattacks are on the rise and, as hackers become more sophisticated, the cost of these attacks continue to grow. Enterprises are acutely aware of these challenges and look to MSSPs to provide security services that offer best of breed protection.

Managed network firewalls are one of the key security services offered by MSSPs but this service needs to be quick to deploy, flexible and profitable. It needs to build on the capabilities you have today so you don't need to retrain your entire team. And it needs to work with your client's existing security tools. We'll show you the foundation for a new push-button managed network firewall service.

Hacker gains access to

100+ million

Capital One accounts in biggest break ever

4.1 billion

records compromised in data breaches in 1H19

Problem

SETTING UP A MANAGED NETWORK FIREWALL SERVICE IS SLOW, CUMBERSOME AND EXPENSIVE

When customers come to an MSSP because they urgently need additional traffic inspection, you want to be able to respond immediately with an implementation that helps them now but can be built upon in the future. But historically, the most common strategy has been to deploy a bigger security appliance per customer. This is slow, cumbersome to manage, and expensive.

Additionally, with a constantly changing IT landscape, evolving network traffic patterns and exponentially growing encrypted traffic, it is difficult to predict the inspection capacity needed in a few months, let alone a year from now. Continuing to add more physical appliances is a never-ending pursuit and it leads one to consider virtualization. It's worked in many places of the network so why not for managed network firewall?

What about a managed service based on virtualization?

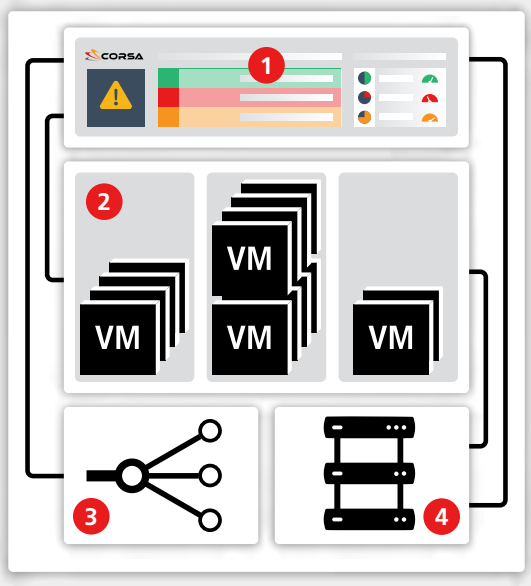
If you go it alone and virtualize threat prevention to offer as a service, in most cases you will keep things simple by buying and maintaining a single virtual machine (VM) per customer, running on a server, with a homegrown hypervisor and mechanism to steer traffic to the VM. If you want better economics, you need to load many virtual firewalls on a single server.

But what happens when you want more than a single VM to build inspection capacity? How do you steer traffic into a new VM? How do you move customer traffic away when a VM's health is not 100%? How do you monitor server CPU and memory resource allocation and adjust? As you can see, this can all create a bigger management nightmare at the network level and for your DevOps team if not done correctly.

Solution

TURNKEY VIRTUALIZATION PLATFORM FOR SCALING TRAFFIC INSPECTION PER TENANT

In principle, virtualization is definitely the right path to take. By distributing virtual firewalls instances across a large number of server CPUs – or security processing nodes - and between any number of servers, you are no longer limited by the performance and management of a physical appliance or a single virtual firewall or a single server. By keeping each virtual firewall's instance small, you are also gaining economic advantages in terms of your licensing costs.



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

Figure 1: Turnkey network security virtualization platform

For a managed network firewall service, you will need to build arrays of VMs with this platform that together create a multi-tenant cluster with the amount (say a few 10 Gbps) of inspection you expect to need. You can then assign portions of this virtual firewall cluster to different customers (tenants) and manage this as a whole.

When all of this is integrated together, it becomes a turnkey network security virtualization platform and it makes it easy to spin up whatever inspection capacity you need, using however many virtual NGFW instances you require, for however many tenants you have signed up for the service. With this tight integration and security orchestration tools, you can manage all those VMs as a unified entity, within the context of your managed firewall service.

Corsa Security platform can be installed in minutes

The turnkey Corsa Network Security Virtualization Platform is pre-built so it can be installed in minutes and your customers never have to deal with the infrastructure. Behind the scenes, the virtual firewall instances are running on state of the art hyperconverged infrastructure (HCI) specifically optimized for in-line network security functions.

By fully integrating with firewall APIs and policy managers, you get a cloud-like user experience for managing the infrastructure and more efficient operations with the Corsa Security Orchestrator. Multi-tenancy allows you to add or remove traffic inspection capacity as needed with the click of a button so you are only paying for the traffic inspection capacity your customers need resulting in better ROI for you.

You can also enable all NGFW profiles

And, when you use a turnkey network security virtualization platform you not only get complete visibility into your customers traffic to better protect their data but you can enable all the NGFW threat prevention profiles without impacting network throughput, including IPS, AppID, Web filtering, SSL/TLS inspection, and more. Each of these can be offered as additional value added services to your clients without having to install yet another appliance.

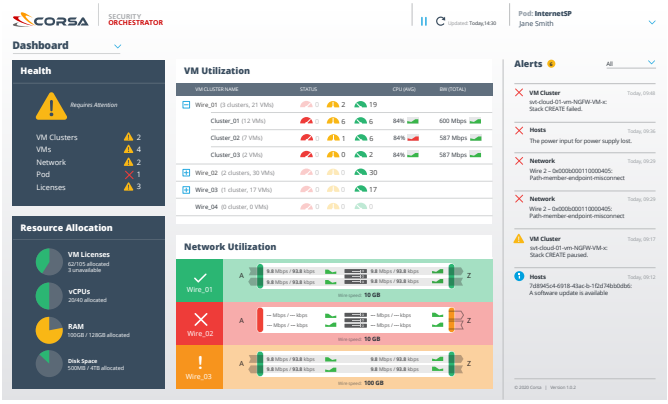
Deployment

A SINGLE PLATFORM THAT SUPPORTS ALL END-CUSTOMERS AND ALLOWS GRANULAR SCALING

The Corsa Security platform is extremely simple to use. From the network perspective it is deployed as a virtual wire firewall. Corsa Security provides all the necessary network, server, load balancing and management components in a turnkey package. You continue to offer your preferred security vendors by providing the appropriate licenses to the virtual firewall instances, and configuring the firewall policy from the existing policy manager.

Managed through a single dashboard

Different client requirements across different sites can be addressed and managed through a single dashboard that is tightly integrated with the firewall policy manager, so the Corsa Security platform can be tuned for customer-specific inspection capacity and threat prevention functions. Therefore, your 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 virtual machines (VMs), you can shuffle VM licenses between clients to allocate inspection where it's most needed. This means you only deploy the exact VM licenses you need at any given time.

No more physical firewalls for each customer

There is no longer any need to deploy new physical firewalls to increase inspection for each customer since with the Corsa Security solution they are collapsed into a single virtualization platform that supports all of the end-customers and allows granular scaling. In some cases, a single VM is enough for the end-customer needs whereas in other cases, a cluster of VMs is spun up to create the required amount of inspection capacity.

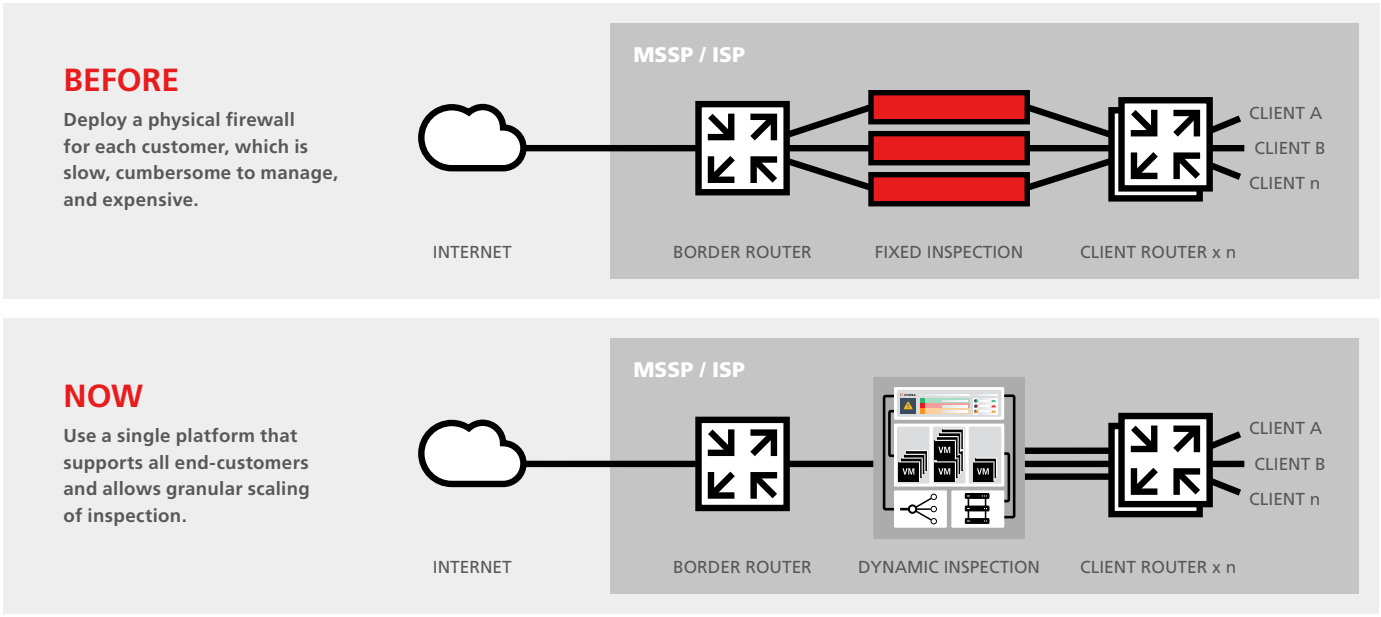


Figure 2: Deploy a single platform that scales inspection to offer the service to all your customers.

Benefits

MULTI-TENANCY FOR IMPROVED EFFICIENCY AND BETTER ROI

With enterprises looking for the latest security solutions and the ability to instantly increase inspection capacity, you have to be able to offer a flexible and up-to-date managed firewall service that protects your customer's network, data and users. This is unsustainable with hardware alone which is why you need to have your managed firewall service use a turnkey virtualization platform for scaling inspection that offers these benefits:

Quick installation

With no hardware to purchase, install, test, or maintain each time, you can install in minutes and dramatically reduce the time you need to turn on more inspection capacity and features for a client.

Stronger security

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

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. And, you can add inspection capacity to new or existing customers without touching routing tables.

Zero downtime

Not only can you support different end-customer inspection requirements, you can scale each of your tenants as granularly as needed and upgrade to new features or services are continuous without needing any downtime.

Better ROI

You deploy only the exact inspection capacity your clients need right now. Your virtualized firewalls are now one large, elastic resource pool instead of many individual appliances so the inspection capacity can be allocated or adjusted as needed one customer at a time.

This platform allows you as an MSSP to offer a new and more flexible service to your customers: complete yet elastic traffic inspection which is tailored to their needs and can scale up or down at any moment. It's also a vendor-agnostic approach, so you can continue to offer the solutions you have today, or work with your client's preferred providers.

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**.