CORSA

USE CASE

Automate your virtualized FWaaS with increased speed, agility, and simplicity

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 virtualized firewall-as-a-service (FWaaS).

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 FWaaS IS SLOW, COMPLEX AND EXPENSIVE

When enterprises come to you because they no longer want to own and manage their own physical firewalls, you want to be able to respond immediately with a virtualized approach that helps them now but can be built upon in the future. But, you need a turnkey solution to automate firewall virtualization so that your customer support team can spin up these services the same-day.

With a constantly changing IT landscape, evolving network traffic patterns and exponentially growing cyber threats, it is difficult to predict the firewall 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.

Why not virtualize the network firewall?

While many enterprises have virtualized their data center infrastructure, it's still not a common approach for network security. Even though virtual firewalls have the same capabilities as their physical counterparts, the network firewall is rarely virtualized. Why is that?

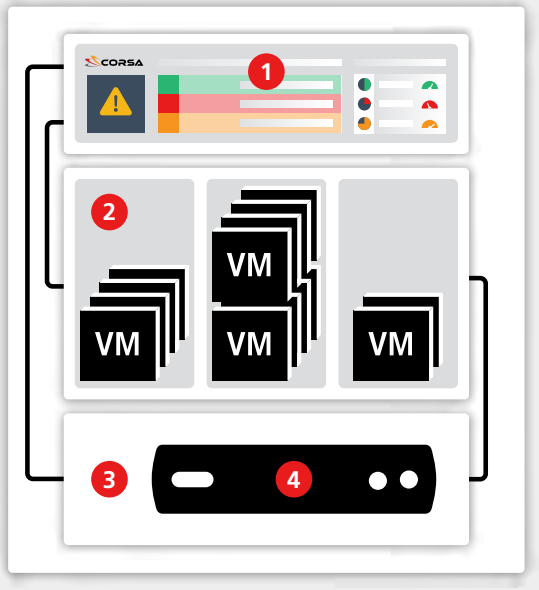
That's because it's hard. If you go it alone and virtualize network firewalls, to offer as a service, there are a lot of things you need to do to build-your-own virtual firewall platform. These include: configuration and optimization of hypervisor software; bootstrap and initially configure NGFW VMs; integration of licensing from firewall vendors; health check mechanisms; maintenance of the platform and much more.

As you can see, this can all create a big management nightmare and requires DevOps resources.

Solution

TURNKEY PLATFORM FOR AUTOMATING FIREWALL VIRTUALIZATION

In principle, virtualization is definitely the right path to take. Your enterprise customers no longer want to deal with the complexity and limited flexibility of hardware firewalls so you can offer them a compelling alternative. A virtualized FWaaS that automatically replaces physical firewalls is the answer.



1. Corsa Security Orchestrator
2. Virtualized firewall
3. Commodity compute servers
4. Hypervisor OS

Figure 1: Turnkey network security virtualization platform for automating FWaaS

For a virtualized FWaaS, you will want to be able to replicate your customer's physical firewalls as installed at the push of a button. Unlike VMWare vRealize and other VM automation tools, this particular automation of firewall virtualization needs to deal with *network* firewalls. This means that network configuration and port assignment is mapped from the physical world to the virtual world and done automatically without any intervention or DIY on your part. And for new customers, you will want to be able to add them quickly and precisely.

Whether the service is for new or existing customers, they can be assigned a share of a virtual firewall (multi-tenancy) or receive a dedicated instance, just like they have for existing services. When they need a change, your support team is now simply adjusting a virtual machine to meet the new requirements.

To accomplish this, you need a turnkey network security virtualization platform that makes it easy to deploy however many virtual NGFW instances you require, for however many tenants you have signed up for the service. With this tight integration of server, hypervisor, firewall VMs and security orchestration tools, you can manage all those VMs as a unified entity, within the context of your managed FWaaS.

Corsa Security Platform can be installed in minutes

The Corsa Security Platform is built on a Secure Access Secure Edge (SASE) framework to converge network and security functions into a unified, virtualized service. It can be installed in minutes and your customers never have to deal with the infrastructure. You can replace all of your customers existing physical firewalls with virtual firewalls that offer the same features but more flexibility.

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 virtual firewalls as needed with the click of a button resulting in better ROI for you.

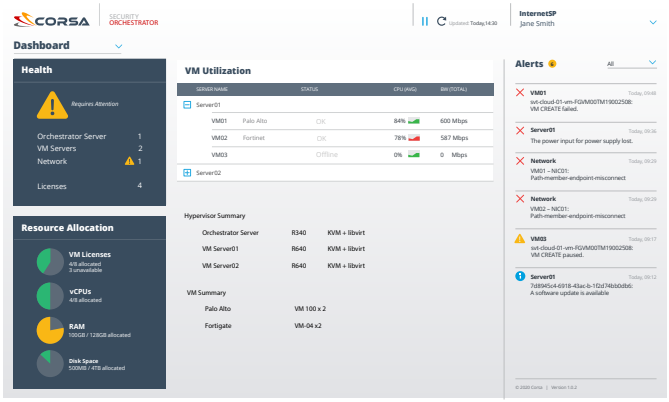
Deployment

A SINGLE PLATFORM THAT SUPPORTS ALL END-CUSTOMERS

The Corsa Security platform is extremely simple to use. Corsa Security provides all the necessary network, server, hypervisor 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 firewall capacity and threat prevention functions. Therefore, your team only has to manage a single configuration, instead of having to source different size firewalls.



Leveraging a single pool of firewall virtual machines (VMs), you can shuffle VM licenses between clients to allocate firewalls 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 for each customer since with the Corsa Security solution they are collapsed into a single virtualization platform that supports all of the end-customers requirements. In some cases, a single virtual firewall is enough for the end-customer needs whereas in other cases, multiple virtual firewalls are needed.

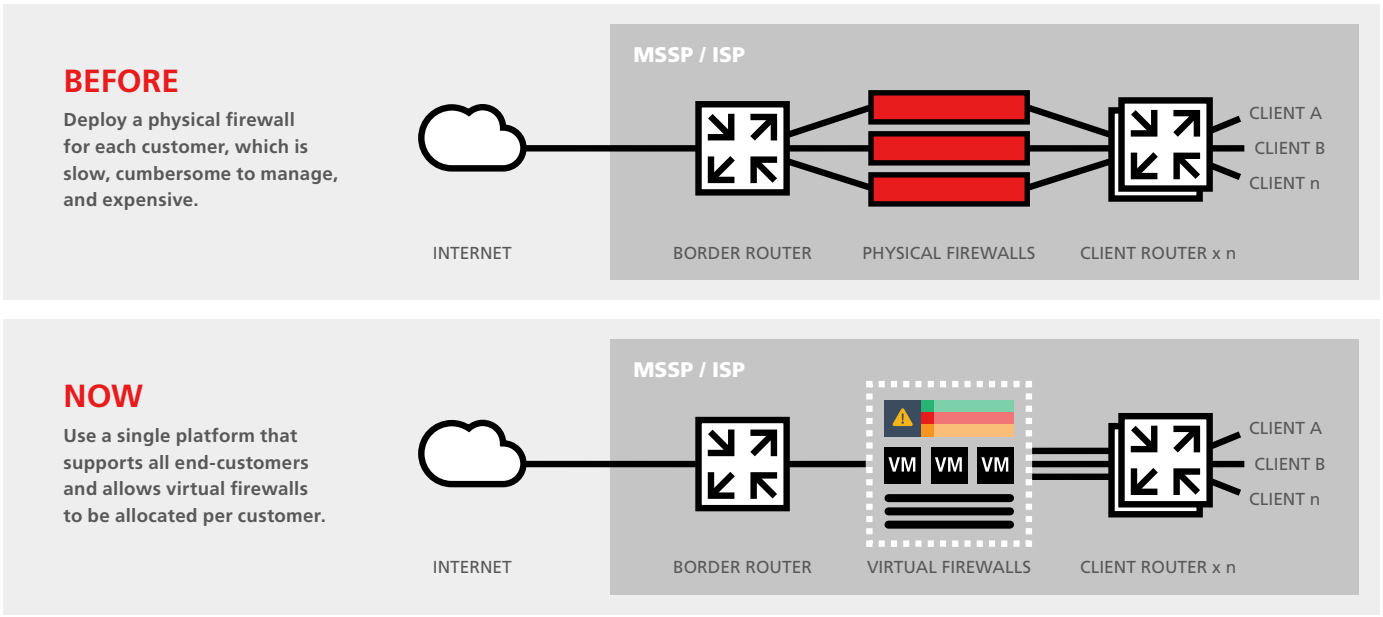


Figure 2: Deploy a turnkey network security virtualization platform to offer a virtualized FWaaS to all your customers.

Benefits

AUTOMATE VIRTUALIZATION FOR IMPROVED EFFICIENCY AND BETTER ROI

With enterprises looking for the latest security solutions and to virtualize their firewalls, you have to be able to offer a flexible and up-to-date FWaaS that protects your customer's network, data and users. This is why you need to have your FWaaS use a turnkey virtualization platform built on a SASE framework that offers these benefits:

Simplify the virtualization of hardware firewalls

You can simplify the virtualization of hardware firewalls with push button provisioning and migration so a customer support team can deploy and execute. It is fully integrated with the firewall licensing and policy management, which is managed through our centralized Corsa Security Orchestrator.

Quickly scale your service offerings

Since the platform supports multi-tenancy, MSSPs can offer specific services and capacity to individual customers in minutes and quickly scale your service offerings. The platform integrates with monitoring, billing, CRM and inventory tools so your team doesn't need to change the way they work.

Reduce network operations expenses for better ROI

By eliminating the need for DevOps skills, offering a low cost of entry and pay-as-you-grow model, MSSPs can reduce their network operations expenses. There is also zero downtime so you do upgrades or add more firewalls whenever your customers need them. Offer your customers a revolutionary new FWaaS with better ROI.

This platform allows you, as an MSSP, to offer a new and more flexible virtualized FWaaS to your customers with increased speed, agility, and simplicity. 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. You get hands-free operations when you virtualize your customers' network firewalls with a pay-as-you-grow model that allows you to quickly scale a successful service.

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 expand traffic inspection, increase threat protection and automate firewall virtualization, at much lower total cost of ownership (TCO). By tightly integrating virtualization with intelligent orchestration, Corsa Security streamlines deployment, management and migration of virtualized next generation firewalls (NGFW) for zero-touch network security operations. Customers subscribe to the Corsa Security services based on their current 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**.