

Five Steps to Automated Firewall Virtualization

How to convert physical network firewalls to virtual ones with increased speed, agility, and simplicity



It is not uncommon for an enterprise to operate their firewall in a **suboptimal manner** and not take full advantage of application-level inspection and filtering capabilities. That's because current firewall architectures are **complicated and expensive**, require **continual monitoring** and lock you in to an **inflexible hardware platform**.

This is why enterprises no longer want to own and manage physical firewalls, but replace them with **virtual firewalls**. But, for this new to be successful, you have to automate firewall virtualization so its **simple, fast and agile**.

Virtual firewall
revenue accelerated

34%

year-over-year
in Q4 2020,



which is significantly
more than the

8%

year-over-year revenue
growth for physical
firewall appliances

Dell'Oro Group

FIVE STEPS TO AUTOMATED FIREWALL VIRTUALIZATION

1 2 3 4 5

EMBRACE
VIRTUALIZATION

DEPLOY A
TURNKEY PLATFORM

SIMPLIFY
YOUR DEVOPS

SCALE YOUR
FIREWALLS

REALIZE
BETTER ROI

EMBRACE VIRTUALIZATION

To keep pace with growing and ever changing cyber attacks, enterprises are learning from the data centers. Instead of trying to manage physical network firewalls, they want to benefit from virtualization to make their network threat protection more flexible and agile to meet these changing demands. A virtualized network firewall eliminates the need for ongoing hardware refreshes to scale capacity, instead giving enterprises an automated, self-service system with pay-as-you-grow capacity. Your team has more time available to focus on high-value, long-term security service innovations that add value to your enterprise.

“

When you adopt **virtualization** to replace physical firewalls, you have a platform that is **more flexible** and can **quickly address new requirements**, both now and in the future.

”

DEPLOY A TURNKEY PLATFORM

But virtualization can be hard. That's why it's important to find a turnkey virtualization platform that is built on a Secure Access Secure Edge (SASE) framework to converge network and security functions into a unified cloud-centric service. When the platform operates as "just-in-time" infrastructure, automating firewall virtualization is simple and quick; it can be done in minutes and if resources become scarce, you are alerted by the system. All it takes is the click of a button to add more firewalls, while the underlying infrastructure remains invisible to your customers. The additional resources are ready for use in minutes as opposed to the days or weeks it takes to set up hardware appliances.

“

By 2024, Gartner expects at least **40% of enterprises** will have **explicit strategies to adopt SASE**, a merger of network and security capabilities into a unified whole.

”

SIMPLIFY YOUR DEVOPS

Many who want to virtualize their firewall architectures are stymied by the time and effort required. There are multiple steps involved 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; and much more. Not to mention the fact that you need to maintain and upgrade this platform. But you can automate the virtualization of physical firewalls with a turnkey platform that takes care of all of these steps so a customer support team can deploy the service and you simplify your DevOps.

“

One of the greatest benefits of automation is **simplicity**. It allows you to **focus** on what sets you apart as a business rather than getting bogged down with menial and repetitive tasks. You gain **increased agility** as well as **costs savings**.

”

SCALE YOUR FIREWALLS

When the firewall virtualization platform supports multi-tenancy, you can offer specific services and capacity to different parts of the network in minutes and quickly scale your security. The platform needs to integrate with monitoring and other security tools so your team continues to use the same processes as they always have except that it's even simpler. And when you need more firewalls or capacity, you can add virtual firewalls in the increments that suit your traffic patterns with the click of a button. There is no more upsizing of hardware firewalls or ongoing hardware refreshes to keep up with network security demands.

“

According to Gartner, firewalls are typically on a **five-year refresh cycle**. For each refresh, organizations need to evaluate everything from throughput capacity to required features and deployment criteria to configuration options.

”

REALIZE BETTER ROI

In the end, the biggest advantage of automated firewall virtualization is significantly higher ROI. Virtual network firewalls need a SASE framework that unlocks operational efficiencies to deliver top rate service velocity. With a turnkey virtualization platform that automates the migration of physical firewalls to virtual, you are not only accelerating your digital transformation but doing so in a new way that will clearly impact your bottom line. By minimizing the need for DevOps skills, offering a low cost of entry and pay-as-you-grow model, you can reduce your network operations expenses resulting in a much higher ROI.

WITH A TURNKEY PLATFORM
AND PAY-AS-YOU-GROW MODEL
YOU GET MUCH HIGHER ROI



Greatly reduced
up-front costs



A future-proof
SASE framework



Operational
efficiencies



Spin up new
services quickly

There is an amazing opportunity to replace your physical firewalls with virtual firewalls. **But you need to automate firewall virtualization through intelligent orchestration for zero-touch network operations.**

A turnkey platform built on a SASE framework quickly and easily lets you automate firewall virtualization that will not only grow your company, but frees up your team to focus on strategic priorities and other new innovations.

**AUTOMATE YOUR FIREWALL
VIRTUALIZATION WITH INCREASED
SPEED, AGILITY, AND SIMPLICITY**

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
or email info@corsa.com

TS-CDD0018-000, Rev 003