CORSA

WHITEPAPER

# Automating Firewall Virtualization is Easy

A turnkey approach helps you replace your physical firewalls with virtual ones

# Summary

Current firewall architectures are complicated, do not scale and lock you in. That's why many people are looking at virtualization to solve the issue just like it did for data centers and the cloud.

However, the thought of virtualization sends shivers down the spine of many a network architect; too many forced virtualization projects gone wrong that lead to costly backtracking and sub-optimal results. But we have learned from these failed projects and the success of the public clouds. The way to make virtualization consumable is to make it automated and deliver it as a service built on a *turnkey* platform.

You have a great opportunity to replace your physical firewalls and begin your enterprise's journey towards a complete secure access secure edge (SASE) architecture. But you need a platform on which to build that service, that offers simple, automated virtualization of hardware firewalls and zero-touch network security operations.

This whitepaper highlights what to look for in such a platform. If you can check off all the boxes in our Turnkey Virtualization Checklist, you'll be very pleased at just how little work it is for you to virtualize your network firewalls.

# Contents


| | |
|---|---|
| Summary | **2** |
| Why Virtualize Network Firewalls? | **4** |
| Offer Virtual Network Firewalls and They Will Come | **5** |
| The Key Elements Needed for Turnkey Firewall Virtualization | **6** |
| The Turnkey Virtualization Checklist | **8** |
| Virtual Network Firewalls with Increased Speed, Agility and Simplicity | **10** |
| About Corsa Security | **11** |

# Why Virtualize Network Firewalls?

It's 2021 and the IT world has gone to "the cloud." But not too long ago the way we built services was quite different. With client-server applications, the standard architecture was to buy physical servers, install operating systems, and then server-side applications.

Then came virtualization. VMware is for the most part responsible for the widespread adoption of the idea that you don't need a dedicated server for a single component of a single application. With virtualization, you can run multiple components or applications on a single piece of hardware.

The next development was Amazon Web Services (AWS). They realized users don't want to spend time doing any of the tasks related to buying hardware or maintaining virtualization software so they made it possible for the service to run in "the cloud" with all of the management and maintenance taken care of for you. And now it's the way of the world. Whether it's public or private cloud, most IT teams have moved past running dedicated hardware for dedicated applications.

In the data center, virtualization has extended to the firewall as well. Virtual firewalls are the deployment of choice in the data center fabric, whether private or public, and, as a result, have evolved to feature parity with their physical appliance counterparts.

Yet despite all this progress with the evolution of virtualization, specifically of virtual firewalls, it is still relatively uncommon for physical network firewalls (those on the North-South links) to be replaced with their equivalent virtual firewall.

Why is that? To move to virtual network firewalls, it needs to be simple to migrate, easy to manage and able to adjust as needed. You must be able to leverage the same type of virtual firewall instances used in the cloud and have an automatic way of creating and deploying exact replicas of the physical firewalls.

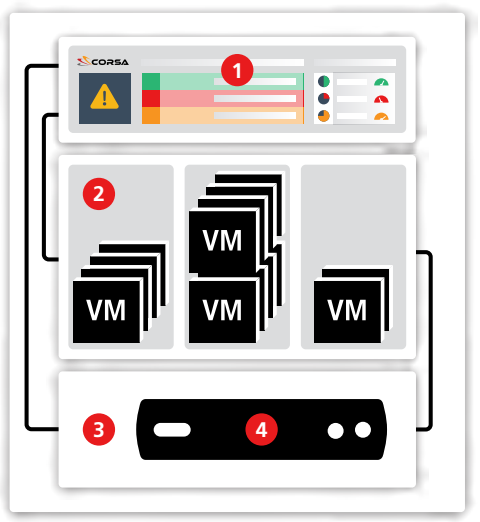
*"To move to virtual network firewalls, it needs to be simple to migrate, easy to manage and able to adjust as needed."*

# Offer Virtual Network Firewalls and They Will Come

The lessons we have learned from AWS, Azure and all the other cloud providers is clear: for anything virtualized to be worth adopting and to consume it as a service, it must be push-button easy. It must be so straightforward that it clearly saves you time and effort and brings you operational and economic efficiencies.

For virtual network firewalls, sometimes called FWaaS, it is no different. It must be completely automated, and tightly integrated with existing network operations. It has to migrate your existing physical firewalls as well as bring up new ones within hours of a service request. And it must be a platform that stands on its own, ready to deploy, without requiring on-going maintenance or heavy lifting.

This is what it means to be turnkey. It can be deployed in minutes and allows you to automate firewall virtualization, while completely eliminating the need to maintain infrastructure.




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

Figure 1: A turnkey virtualization platform for automating firewall virtualization

# The Key Elements Needed for Turnkey Firewall Virtualization

There are a number of crucial elements to a turnkey solution that automates virtual firewall creation, thus freeing up your time to focus on other more strategic customer needs instead of infrastructure.

Up front, this form of network firewall virtualization has considerations that are different from virtualizing web applications. Unlike VMWare vRealize and other virtual machine (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, for example. For a turnkey virtualization platform, these requirements include:

**Turnkey makes sure you use the right commodity server for the virtual firewalls to run on.** Network security functions as a workload are vastly different than a typical enterprise application. Next generation firewall (NGFW) appliances normally use purpose-built ASICs for network security, thanks to the hardware acceleration they provide. With virtualization you would want to run your virtual firewall instances on general-purpose x86 CPUs, which is great on the budget but they're typically not optimized for network security. So to get optimal, predictable and on-par performance from your compute, you need a good understanding of the server architecture to avoid bottlenecks of network I/O between the NICs, the CPUs and the RAM inside the server.

**Turnkey provides hypervisor software on the server.** Again, most current hypervisors and related software are not designed for firewall functions. So you need one that is suitable while considering all the relevant networking acceleration technologies – such as SR-IOV, DPDK, and others – that helps you get the most performance out of the selected server hardware.

**Turnkey automates the bootstrap, upgrade of software, and configuration of the virtual firewall.** Booting a firewall VM on top of your hypervisor involves a huge amount of DevOps resources. After the VM has booted up, it isn't ready to go straight away. You need to apply the appropriate license to it. And, once the VM is licensed it still needs to get its settings and policy configuration. Typically, this is done either manually by logging into the user interface (UI) of the VM, or from the centralized policy manager. In order to be truly cloud-like, all this needs to happen automatically. So it's not just the integration of the 3rd party firewall vendors' firewall VMs with hypervisor and server that must be taken care of but also the integration with the centralized policy manager.

**Turnkey scales across multiple firewalls.** It allows you to create as many virtual firewalls as you need. It supports multi-tenancy as well as multi-vendor on a single platform.

Ultimately, the expectation of this turnkey firewall virtualization is automation so you get agility, flexibility and elastic capacity. And this is what has been outlined so far.

In order to maintain and manage this combination of virtual firewalls, the turnkey virtualization platform must also incorporate orchestration so it all works together and is controlled by a single dashboard. This orchestration must provide full management and configuration of the whole platform and be tightly integrated with the firewall vendor's licensing application programming interfaces (APIs) and policy managers.

You also want to make sure it offers full zero-touch auto provisioning and built-in health check mechanisms to monitor VM health so you can eliminate DevOps resources to manage the virtual firewalls.

It's a lot to develop up front and then maintain going forward, which is why a DIY approach often fails or ends up costing a lot. But if you use a turnkey platform you can automate the migration of physical to virtual firewalls for your enterprise customers and move them to the cloud centric service they ultimately desire.

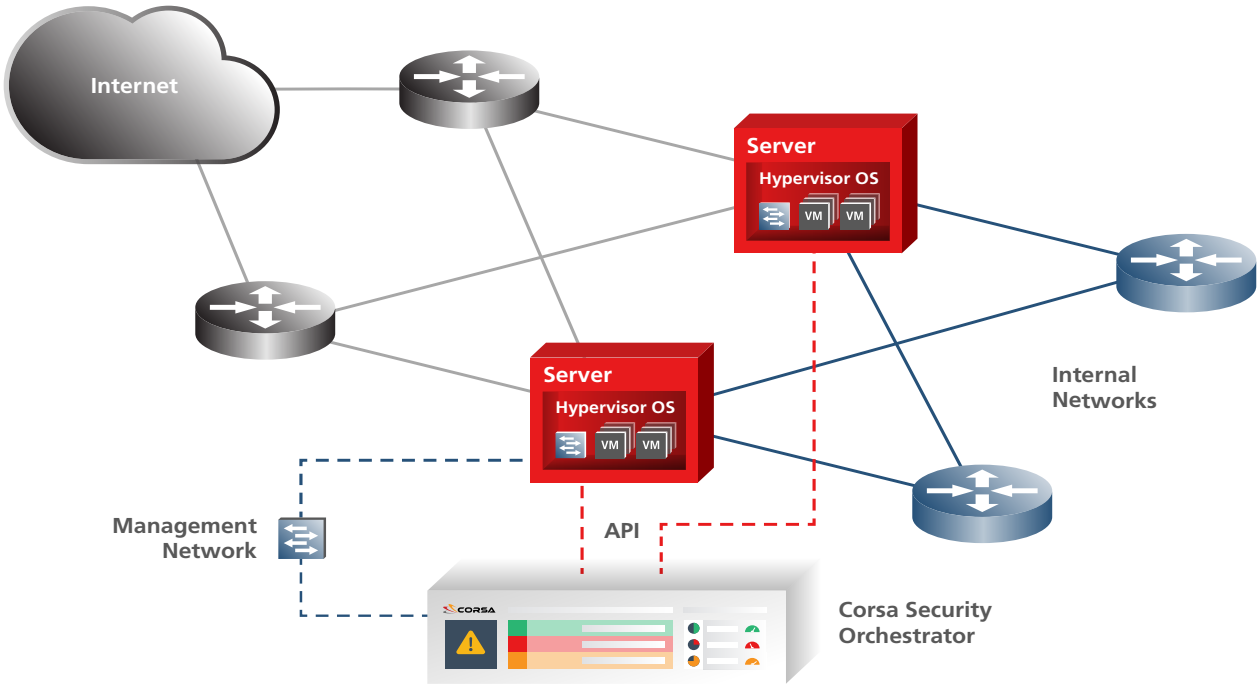



Figure 2: The turnkey virtualization platform must be delivered as a ready-to-deploy service

# The Turnkey Virtualization Checklist

Can you imagine using Google Cloud if you had to specify which server you were going to use and what kind of SR-IOV optimization you wanted? Or if you had to upgrade the hardware at some point? No way, it defeats the purpose.

Your managed network firewall service running on virtual firewalls needs to be available as a readily consumable service to be successful. All the great cloud platforms that exist today have accomplished this. For virtual network firewalls, you need a turnkey virtualization platform to make this possible.

All of the elements of turnkey virtualization were discussed in the previous section. Now you can use this checklist to review if a platform is actually delivering. Review each item and consider it on its own but more importantly review how each item is integrated into a whole platform. Integration of all the pieces is far from trivial and rapidly gains more complexity as you scale your needs. When it's a turnkey platform, this is all dealt with for you.

| **Steps To Build and Maintain Your Firewall VM Platform** | ☑ Specification and purchase of server hardware optimized for network security | ☑ Configuration and optimization of hypervisor software for firewall virtualization | ☑ Orchestration and automation to Bootstrap& initially configure NGFW VMs |
|---|---|---|---|
| ☑ Integration of licensing from vendors into the orchestration and automation | ☑ Provisioning of configuration and policy settings to the VMs in a zero-touch way | ☑ Health check mechanisms to monitor VM & system performance | ☑ Automation of firewall configuration migration |
| ☑ Single-pane-of-glass VM orchestration & monitoring GUI | ☑ Testing and validation of firewall VM platform | ☑ Maintain platform compatibility with firewall VM revisions | ☑ Maintenance of platform |

Table 1: The turnkey checklist for automating firewall virtualization

With a turnkey platform, you save time and money by not needing DevOps – no team of engineers who will have to specify and source the appropriate servers, no experts to code up an integration of the servers with management of the virtual licenses. And no need to blend those scarce skills with an understanding of networking so that traffic is properly handled and inspected, while being managed by the security policy manager.

You are also divorced from managing infrastructure and therefore save yourself the big, fat perennial headache of managing vendors and integration. With a turnkey approach, you don't have to deal with different vendors' products and there's no need for professional services and support from each of them, never mind all the procurement and testing.

Moving to a turnkey platform dramatically reduces project risk and speeds time to deployment. You reap the benefits of the SASE model for the modernization of your network.

*"Moving to a turnkey platform dramatically reduces project risk and speeds time to deployment."*

# Virtual Network Firewalls with Increased Speed, Agility and Simplicity

A turnkey platform revolutionizes how you deploy and manage your firewalls. In the past, it involved deploying multiple physical firewalls, managing them and replacing them when you needed more capacity. This could be very resource intensive. If you deploy a turnkey platform that meets the checklist requirements above, this is no longer the case. The platform will deliver these key benefits:

## Simplify the virtualization of hardware firewalls

You can simplify the virtualization of hardware firewalls with push button provisioning so anyone on the IT team can deploy and execute. It is fully integrated with the firewall licensing and policy management while offering automatic migration.

## Quickly scale your firewalls

Since the platform supports multi-tenancy, you can deploy specific services and capacity to different networks in minutes and quickly scale your firewalls. When the platform integrates with monitoring and other security tools, your team doesn't need to change the way they work.

## Reduce network operations expense for better ROI

By eliminating the need for DevOps skills, you can reduce your network operations expense and realize better ROI. There is also zero downtime so you do upgrades or add more firewalls whenever you need them.

---

**A turnkey platform allows you to deploy and manage virtual network firewalls with increased speed, agility, and simplicity. It's also a vendor-agnostic approach, so you can continue to use the solutions you have today, or work with other preferred providers. You get hands-free operations when you virtualize your network firewalls to quickly scale security as needed.**

---

# 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.

## Please contact us

For more information about our solutions,
please contact Corsa today.

84 Hines Road, Suite 100
Ottawa, ON Canada  K2K 3G3
613 287 0393

sales@corsa.com
www.corsa.com

CORSA