TCO of Virtual On-premise Firewalls

CALCULATING THE COST SAVINGS AND OTHER BENEFITS WHEN YOU AUTOMATICALLY DEPLOY, SCALE AND OPTIMIZE VIRTUAL FIREWALLS

Current firewall architectures are complicated, do not scale and lock you in. That's why many organizations are looking at firewall virtualization. But it takes a lot of time, resources and specialized skills to convert physical to virtual firewalls and then efficiently scale and optimize your virtual firewall environment.

By tightly integrating virtualization with intelligent orchestration in a single UI, you can save time and money by minimizing the need for DevOps while reducing project risk and speeding up time to deployment. You are also divorced from managing physical firewall infrastructure and therefore save yourself the perennial headache of frequent RFPs for firewall refreshes.

Let's look at the benefits of virtual firewalls versus physical ones and then the costs of various approaches.

BENEFITS OF VIRTUAL FIREWALLS VERSUS FIREWALL APPLIANCES

The benefits realized by using virtual firewalls with intelligent orchestration that automates firewall virtualization are significant and outlined in the table below as they compare to the hardware-based firewalls.

Benefits	Firewall VMs with Intelligent Orchestration	Firewalls Via Hardware Appliances
No need to tie up engineering resources. Customer or IT support can add firewall capacity for a new customer or user in minutes.	☑	☒
Zero-touch provisioning meaning no hardware to cable it's all software to call up new virtual firewalls, shuffle virtual firewalls, add firewall services and subscriptions to existing customer accounts.	☑	☒
No outdated appliances. Since VMs are a pooled firewall resource, it's easy to replace VMs with new ones – always with the latest software version.	☑	☒
Zero downtime for any firewall during upgrades because upgrades are continuous.	☑	☒
Burst firewall capacity can be added with the click of a button and if you are an MSSP it can now be metered and charged for.	☑	☒
Cost-efficient pay-as-you-grow firewall capacity model so MSSPs and enterprises only pay for the capacity they need.	☑	☒
No need to share firewalls since each tenent gets dedicated virtual firewall with specific security services and subscriptions per their requirements.	☑	☒
No need to manage a whole variety of different firewall models and instead gets an elastic, pooled firewall resource consolidated around one platform.	☑	☒
Ends the process of having to do firewall refreshes every few years. Instead, just add what is needed, continuously, with all the latest upgrades/subscriptions included.	☑	☒

About Corsa Security

Corsa Security is the leader in automating network security virtualization, which helps large enterprises and service providers deploy, scale and optimize virtual on-premise firewalls with speed (24x faster deployment), simplicity (zero-touch operations) and savings (9x lower TCO). By tightly integrating virtualization with intelligent orchestration in a single dashboard, the Corsa Security Orchestrator provides an aggregated view of all your virtual firewall while managing the infrastructure health, capacity, and performance. Customers subscribe to the Corsa Security services based on their current needs and then pay as they grow by integrating credit-based licensing from our firewall partners. Learn how Corsa is revolutionizing network security at corsa.com.

THE SAVINGS ADD UP WITH AUTOMATED NETWORK FIREWALL VIRTUALIZATION

There are many steps and workflows needed in a system that converts your physical firewalls to virtual equivalents and then scales and manages them. Each step requires development from a team of experts in network engineering, security, systems integration and DevOps. And once the system is developed, on-going maintenance, upgrades, testing and validation are required which are a huge drain on resources.

To tackle all of this with a DIY approach can be a huge roadblock. By tightly integrating virtualization with intelligent orchestration, all of this is taken care of and you are able to instantly activate your new firewall services as needed.

Steps To Build and Maintain Your Firewall VMs	Specification and purchase of server hardware optimized for network security	Configuration and optimization of hypervisor software for firewall virtualization	Orchestration and automation to Bootstrap and 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
	$500,000 to purchase	**400 hours** to build functionality	**250 hours** to build functionality	**150 hours** to build functionality	**200 hours** to build functionality
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
200 hours to build functionality	**2,000 hours** per year	**800 hours** to build functionality	**600 hours** to build functionality	**300 hours** per year to maintain compatibility	**2,000 hours** per year
					6,900 Hours Total

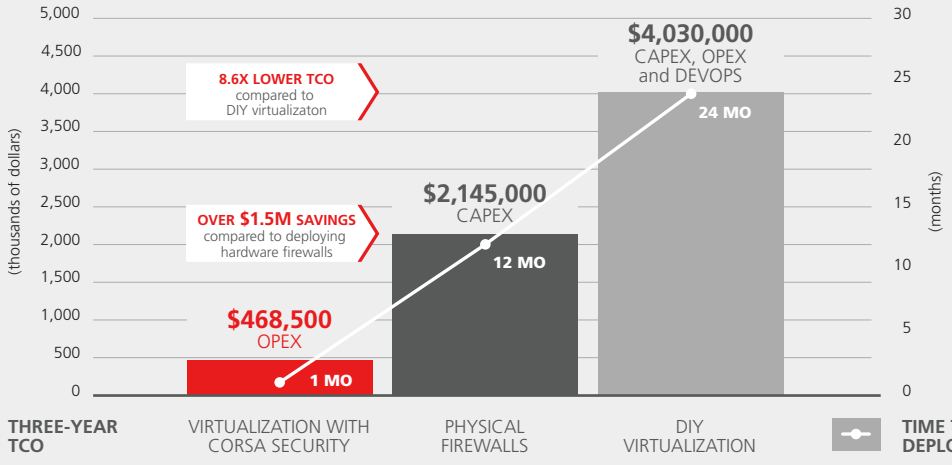
THREE-YEAR TCO ANALYSIS: PHYSICAL FIREWALLS VS AUTOMATED FIREWALL VIRTUALIZATION VS DIY FIREWALL VIRTUALIZATION

For our TCO scenario, we look at a network deployment that needs 50 firewalls and explore whether they should deploy physical or virtual ones and then whether virtualization can be done cheaper in-house. To go the hardware-based firewall route, they need to buy 50 physical firewalls with the appropriate license for 3 years plus 3 years of support. **This will cost $2,145,000 CAPEX up-front and take over a year from conducting the RFP process to deploying the firewalls.**

If they want to go the virtual firewall route, and think they have the expertise in house to try it, we can use the table above to calculate the costs of the equipment plus the time spent by their team to build a virtualization platform. Based on our estimates, this will cost $500,000 up-front for equipment plus between $1,720,000 to $2,150,000 in resources to build and deploy the solution. There will also be ongoing support and maintenance of $345,000 to $460,000 per year. **The total cost over 3 years will be $3,255,000 to $4,030,000 and it may take over 2 years to build the platform before you get started.**

To leverage intelligent orchestration for automated firewall virtualization, like the Corsa Security Orchestrator software, you will need to sign up for a monthly subscription but no longer need to worry about the CAPEX for hardware, pay-as-you-grow and have the flexibility of a common platform for different firewalls rather than being locked into the hardware you purchased in option 1. **The total cost of this route is $468,500 OPEX over 3 years and you can be up in running in 30 days or less.**

8.6x lower TCO and 24X faster time to deployment



YOU CAN SAVE OVER 78% AND DEPLOY 12X FASTER
if you deploy virtual on-premise firewalls compared to hardware firewalls plus you eliminate up-front CAPEX.

BUT THIS IS NOTHING COMPARED TO THE ALMOST 9X LOWER TCO AND 24X FASTER TIME TO DEPLOYMENT
with intelligent orchestration instead of DIY virtualization.