www.pipelinepub.com
Volume 19, Issue 1

A Simpler and More Profitable Firewall Service

By: Carolyn Raab

With the number of cyberattacks growing and hackers becoming more sophisticated, the cost and complexity of network security is increasing. Enterprises are acutely aware of their need for best-in-breed threat protection, but they don't want the complication and expense of dealing with hardware appliances that lock them in and don't scale. Instead, they want a firewall service that is easier to manage while also offering the latest security solutions.

Service providers (SPs) and managed security service providers (MSSPs) are uniquely positioned to solve these challenges by offering managed virtual firewall services. In such a competitive environment, however, they need to be able to deploy these services without exponential increases to capital or operating costs. This article explores how virtual firewalls deliver the flexibility, scalability, and agility a growing enterprise needs in today's cyber landscape. It also lays out two crucial characteristics this virtual firewall platform needs to have to be a profitable and effective service offering.

The business case for virtual firewalls

Deploying a managed network firewall service is typically a large drain on finances and engineering resources. Hardware appliances are slow, complex, and expensive to set up. They are cumbersome to manage, need replacing every few years, and might not be able to keep up with the frequent changes in security needs from the enterprise. This is why the introduction of a hosted, managed virtual firewall service (VFS) is a compelling alternative for SPs and MSSPs.

Virtual firewalls offer the same features as physical ones, but with the flexibility enterprises need these days. If you offer a managed VFS, you no longer need to deploy physical firewalls every

time you onboard a new customer, or whenever an existing customer needs additional capacity due to a new office location or new employees. When your customer needs a change, your customer support team simply deploys a new virtual firewall with the click of a button to meet the new requirements. A virtualized approach helps your customers now ***and*** can be built upon in the future.

This sounds great in theory, but for it to be as profitable as possible, there are several criteria such a service needs to meet. The technology needs to deliver the service to customers whenever and wherever they want. It has to enable same-day delivery of new firewalls when onboarding new customers to the service. It needs to reduce operating costs by transforming the process of adding threat protection capacity for a customer from an engineering to a customer support function. And, you'll want pay-as-you-grow flexibility, so you are not making unused investments in firewall hardware.

This is a long list—and if you were to build it from scratch, you would end up draining your engineering resources and budget. You would be back to square one: an expensive, complex network firewall service. In order to make the most of the advantages of virtual network firewalls, there are two factors you need to leverage: ***automation*** and ***intelligent orchestration***. It's these two factors that will make the difference between a complex, expensive managed security service and an easy-to-manage, profitable one.

Automated firewall virtualization to migrate physical firewalls

DIY virtualization requires extensive engineering resources. You need the expertise and time to take care of many tasks: configuration and optimization of hypervisor software; bootstrapping and initial configuration of NGFW VMs; integration of licensing from firewall vendors; health check mechanisms; maintenance of the platform and much more. Why should an MSSP take that engineering headache from their customers only to add it to their own plate? It doesn't make sense. Automation, on the other hand, delivers higher accuracy, greater uniformity, and simpler workflows. When

automation is baked into your managed VFS, the migration of firewalls from physical to virtual is quicker and more reliable—you don't have to devote hours of engineering expertise or worry about human error. As well as automated deployments, you get push-button provisioning. In other words, the scaling and optimizing of on-premise virtual firewalls happens automatically, meaning your customer support team can spin up these services the same day without in-depth training or engineering capability. Provisioning and management are cloud-like, creating an intuitive and familiar UI that simplifies all the complex operations your support team must take care of.

Intelligent orchestration to transform your environment

There is one other factor you need for your new firewall service to be simpler and more profitable—intelligent orchestration. Intelligent orchestration is a powerful tool that allows you

to visualize and control your virtual network firewalls across all on-premise environments. It **automates** the full lifecycle from deploy to scale to optimize, including licensing, zero-touch deployment, maintenance, troubleshooting, and machine intelligence.

The ability to view all resources in a single UI gives you end-to-end visibility and control from one console. It serves up a consolidated view of all the compute servers and virtual machines and their state, for example: the overall health of the system, server resource allocation, VMs and network utilization. The "intelligence" comes from the recommendations on the best allocation of virtual firewalls in the context of your entire deployment, including automated scaling.

Intelligent orchestration makes it very simple to add new virtual firewalls, change existing ones, and adjust resources without the need for additional DevOps work. This enables IT teams to automate tasks across multiple platforms, making your team nimbler when responding to change. And it brings predictability to managing the virtual infrastructure in your clients' networks.

The benefits of a hosted managed virtual firewall service

When SPs and MSSPs offer a hosted managed VFS, they gain incredible service velocity, agility, and profitability. With automation and intelligent orchestration, you can add or remove virtual firewalls as needed with the click of a button, so your network firewall service becomes a quick and easy customer support function instead of a big engineering project. And with multi-tenancy, you get flexibility and portability across environments for an even more agile service.

But it's not just about speed and agility; you can also reduce your network operations expenses, resulting in a better ROI. First, you don't have to invest in physical hardware, or the licenses and support over the life of the hardware. Second, you save on costly and scarce DevOps resources to develop, test, and maintain physical hardware, or to complete a DIY virtualization project. Finally, with a pay-as-you-grow model that optimizes credit-based licensing, you only pay for the capacity and firewall licenses you need, and you don't have to plan overcapacity into your purchases or architecture.

Enterprises are looking for a firewall service that can effectively protect them from the latest cyberattacks today and grow with their organization's ever-changing needs, without draining engineering resources or their bank balance. Service providers and managed security service providers have an opportunity to plug the gap by taking this engineering headache from their customers with a hosted managed virtual firewall service. The key is to leverage the benefits of automation and intelligent orchestration so that this new virtualized service is quicker to deploy, offers more agility and delivers increased profitability—all while delivering best-in-class threat prevention.