vmware

Customers' Security Challenges, and VMware Firewall-as-a-Service

A Natural Partnership >

The opportunity: Safeguard your customers, unlock new revenue streams

Lack of effective security is the number one reason enterprises decide not to use a managed cloud service, according to IDC[1]. So there's a great opportunity, right now, for VMware Service Providers like you to offer zero trust firewall-as-a-service, in order to:

- Wrap your customer services in best-in-class protection, removing barriers to customer adoption, and helping you stand out from your competition.
- Upsell virtual firewall services that help you capture a bigger share of your customers' overall IT security spend.

25% of businesses increased their security investments in 2020,[1] with spending on cloud security increasing 33%.[1] So there's a fast-growing addressable market waiting for you to take advantage of.

Firewall services for the digital world

VMware recommends that offering each customer physical perimeter-based firewalls may not be necessary. Instead, offering a distributed 'zero trust' approach that protects each workload at the application level, no matter where it resides, is an ideal complement or alternative to a physical firewall.

As customers embrace digital transformation, typically using a blend of on-prem and cloud-based workloads, services based on distributed firewalling will give your customers the hybrid protection they need.

These capabilities are already at your fingertips, with edge firewalling included in your 7pt Flex core. Plus they're easy to deliver with VMware Cloud Director and fully-integrated VMware NSX-T.

Why look again at Firewall-as-a-Service?

Traditional physical perimeter firewalling, patching, and 3rd party virtual firewalling can easily fall short when it comes to protecting today's hybrid workloads:

- Traditional DMZ security architectures that focus on perimeter security are complex and costly to manage and configure; and they offer no protection against threats that penetrate the perimeter.
- Routing traffic between applications via a perimeter firewall ('hairpinning') is inefficient, unnecessarily increasing traffic.
- Customers will struggle to keep pace with technology, which means that in future, 99%[2] of all firewall breaches will be caused by misconfigurations, not flaws, requiring automated policy controls to support increased volume and growth.

The solution: Firewall-as-a-Service on VMware NSX-T

VMware NSX-T enables Service Providers to protect individual virtual workloads in – and as they move within – a VMware environment.

This distributed firewall functionality is underpinned by NSX virtual networking, so any virtual networks you create for customers using NSX are, by default, isolated and secured from each other.

This provides protection, isolation and segmentation of East-West traffic within the data center environment, protecting individual VMs and their data and applications against threats like worms, Trojans, viruses and malware from spreading unchecked. Without visibility of East-West traffic, threats that penetrate the perimeter firewall can move unchecked around the network. **Yet even in 2020, as little as 10% of East-West traffic ever sees a security control.**[3]

Just as important, it enables automated and bespoke firewall and security policies to be enforced at individual workload level, according to each customer's individual security, compliance and governance priorities.

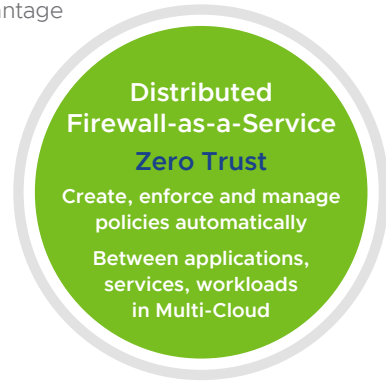
How you benefit

Once you virtualize a customer's network with NSX, you can:

- Run customer workloads that belong to different customers and different zones on the same hypervisor clusters, achieving much higher consolidation ratios without compromising on security.
- Increase your margin by automating security services: Service Providers have successfully reduced cycle times by 90%, and task effort by 80%, with NSX.[3]
- Consolidate or reduce physical appliances to achieve an estimated 25% CapEx saving.[4]
- Offer enhanced Layer 7 application-level security to give customers visibility and protection.
- Maximize the operational simplicity and compliance of your firewall services, and offer them to your customers as either managed services or on a self-serve basis.

Remember, robust security is customers' #1 demand when they invest in cloud services. So give them peace of mind by demonstrating how you'll protect their workloads with modern, fit-for-purpose distributed firewalling.

By helping you take advantage of this relevant market opportunity, in a way that's profitable and differentiated from your competition, we're continuing to demonstrate our commitment to supporting our Service Providers in a true spirit of partnership.



Learn more about Firewall-as-a-Service with VMware NSX

Download the IDC white paper >

1 Buyer Requirements for Managed Cloud Services and Expectations of Managed SPs Feb 2020. 2 Source: VMware. 3 Source: www.lastline.com/blog/why-monitoring-east-west-traffic-is-crucial-for-cloud-security. 4 Replace physical appliances and save ~25% over CapEx cost/8yrs. Source: VMware.

A Natural Partnership <

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com