White Paper: **September 2021**

Internal Firewall: The Best Way to Protect East-West Traffic

Table of contents

IT security professionals want application-centric, built-In, cross-platform security control[1]

- Approximately half are managing more than 20 agents.
- 60 percent prefer built-in security controls over agent-based solutions.
- 70 percent agree security controls should be built in to the hypervisor.

Introduction

Even in the best of times, chief information security officers (CISOs) and their teams face numerous challenges in protecting the brand, the business and sensitive data against ever-changing threats—all with finite and constrained resources. Today, those challenges are more extreme than ever. In a rapidly changing world, CISOs need a way to defend the growing number of dynamic workloads and increasing internal network traffic against cyberattacks.

Traditional security approaches are not the answer. Bolted-on security solutions can't deliver the scalability, flexibility and cost effectiveness needed by today's security teams. Instead, enterprises should insist on intrinsic security—security built in to the infrastructure, distributed and application aware.

This white paper explains why intrinsic security, in the form of a Distributed firewall, is essential for protecting the brand. It highlights three examples of how VMware customers use the VMware Distributed Firewall to mitigate risk, comply with policies and standards, and improve agility while scaling seamlessly and cost effectively along with the business. The Distributed Firewall is a distributed, scale-out internal firewall that protects all east-west traffic with security that's intrinsic to the infrastructure, radically simplifying the deployment model.

Protecting the brand with intrinsic security

CISOs aren't the only ones dealing with the pressures of rapid change. Software engineering teams are tasked with continuous innovation and expected to deliver new features and new code deployments weekly or even daily. To achieve this level of agility, application architectures shift from a monolithic approach (where changes require redeploying the entire application) to a distributed one (where changes can be made quickly to small, independent services without having to redeploy the entire system). In a distributed architecture, each application becomes a network unto itself, with communication in the form of network traffic between different workloads and microservices.

Network security controls invented in the era of monolithic applications or even three-tier applications are no longer adequate to protect present-day application infrastructure. Traditional security controls lack awareness of intra-application traffic flows. As application infrastructures evolved, security teams added more security tools to try to protect dynamic workloads, which led to tool sprawl, higher total cost of ownership, operational complexity and the need to trade necessary security controls for speed to market when it came to new capabilities.

For all these reasons, security organizations began adopting a far more effective approach to securing workloads and sensitive data: intrinsic security. Built in to the IT architecture instead of being bolted on, intrinsic security is distributed, application aware and simple to operate.

[1] Forrester Consulting. "To Enable Zero Trust, Rethink Your Firewall Strategy." February 2020.

Further reading

To learn more about the challenges of traditional network security controls for protecting modern workloads, read Five Critical Requirements for Internal Firewalling in the Data Center.

An internal firewall with intrinsic security, like that from VMware, protects workloads while eliminating the complexity and expense of multiple, bolted-on security solutions. The VMware Distributed Firewall—which includes a distributed firewall, an intrusion detection system and intrusion prevention system (IDS/IPS), and deep analytics through VMware NSX® Intelligence™ (see Figure 1)—improves the security of today's modern workloads. It helps CISOs and their teams protect the brand, the business and sensitive data against cyberthreats by mitigating risk with an intrinsic security approach that enables compliance, and simplifies and scales operations cost effectively and without compromising security.

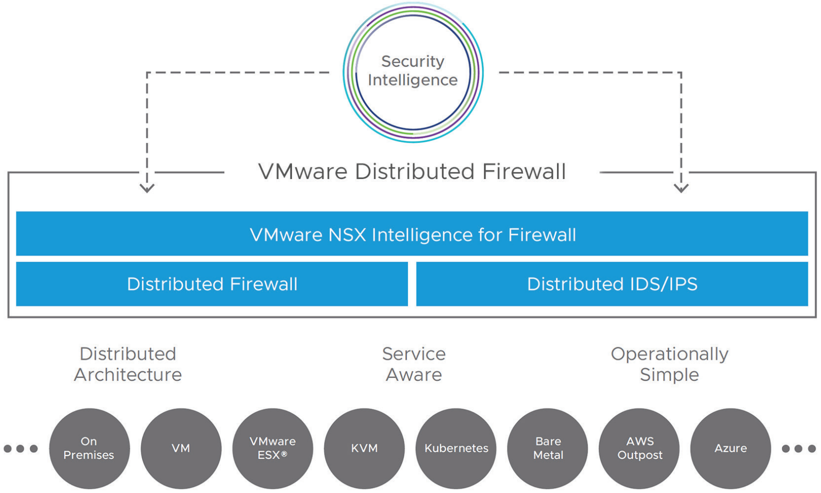

FIGURE 1: The VMware Distributed Firewall.

Mitigating risk

The traditional castle-and-moat perimeter security model is inadequate for protecting modern IT environments. Instead, new approaches such as zero trust call for monitoring and protecting traffic within the data center on the principle that no traffic should be trusted until policy proves otherwise.

Micro-segmentation is one of the core concepts within the zero-trust model. It involves isolating workloads from each other and securing each of them individually. For organizations with large numbers of applications and workloads, segmentation is often implemented incrementally, starting with macro-segmentation of specific environments (such as development from production), then with micro-segmentation of the virtual desktop infrastructure or other single application environments, and finally with micro-segmentation of all applications.

An internal firewall is the most efficient and effective way to deploy network segmentation in support of a zero-trust approach because the firewall can:

- Analyze every packet and workload in east-west (internal) traffic to detect and block threats.

- Use deep application awareness and visibility alongside detailed identification of application topology to monitor all traffic flows.
- Provide granular control at the service level with automated policy recommendations.

Customer experience: Deploying micro-segmentation in a financial institution

A large financial institution that offers banking and other financial services to more than 30,000 customers and manages more than $800 million in assets wanted to move to a zero-trust security model to better protect customers' personal and financial information. The CIO made the decision that all traffic, including all east-west (internal) traffic, would be secured. To effectively adopt zero trust, the financial institution needed a way to:

- Easily segment applications to prevent the lateral movement of threats.
- Minimize the expense and burden of a zero-trust deployment on the five-person security operations team.
- Accommodate potential future use cases, such as edge services and multi-cloud environments.

The financial institution chose the VMware Distributed Firewall to enable micro-segmentation of all applications to block lateral movement of cyberattackers. In a matter of weeks, the security operations team went from planning to production with its first micro-segmented application. In a few months' time, the team discovered and secured all applications within the data center.

Using the Distributed Firewall, the security operations team was able to implement zero trust quickly throughout the entire environment while keeping costs low by automating network and security configurations. Standardizing on the Distributed Firewall allowed the financial institution to remove multiple legacy tools, use a single pane of glass for security management and significantly improve the IT team's operational efficiency while mitigating risk.

Enabling compliance

Not only do companies need to comply with all applicable laws, rules and regulations, but many organizations also have internal rules, policies and procedures that must be followed. Whether it's a mandate—such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) or the Sarbanes-Oxley Act (SOX)—or internal rules and regulations, CISOs and their teams have to implement and enforce compliance requirements.

Meeting compliance requirements necessitates the ability to create and propagate specific security policies to all relevant workloads, and track traffic flows to and from sensitive applications. An internal firewall eases the cost, complexity and effort of compliance while fulfilling security requirements by:

- Tracking and inspecting all traffic to and from sensitive applications to eliminate blind spots
- Streamlining the creation and customization of multiple, virtual security zones for sensitive applications
- Automatically creating, distributing, moving and decommissioning policies according to each sensitive workload's lifecycle

Customer experience: Securing electronic health records for regulatory compliance

To comply with HIPAA, a large health system with thousands of physicians and nurses needed to implement and enforce fine-grain access controls to protect patient data within its electronic health record (EHR) system. Traditional, hardware-based firewalls would not be able to scale to accommodate the rules required and would create management complexity as rules needed to be changed.

If the health system used its perimeter firewall as an internal firewall, the health system would need to manually create new security policies and modify them whenever a workload was moved or decommissioned, which could lead to potential configuration errors and take time away from other security efforts.

With the VMware Distributed Firewall, the health system moved from design to production in just six weeks. The security team used the internal firewall from VMware to segment and protect the EHR system with granular security policies automatically propagated to all relevant workloads. The internal firewall now tracks all traffic flows to and from the EHR.

After deployment, the health system experienced a ransomware attack but, because each of the subcomponents of the EHR application was secured by the Distributed Firewall, the system blocked the lateral movement of the threat into the EHR environment. The EHR application and sensitive patient records remained protected from and unaffected by the attack.

Simplifying security architecture, scaling operations and supporting business agility

As more monolithic applications are replaced with or rearchitected into distributed applications, the number of workloads and the volume of traffic between those workloads has increased exponentially. Security teams need a way to keep up with the speed of development and the pace of the business. To gain this agility, internal firewalls must be easily scalable and simple to manage to efficiently protect the growing number of workloads—and the brand.

CAPEX savings

By implementing the VMware Distributed Firewall, enterprise customers could see a reduction of up to 60 percent in the number of traditional firewalls required.[2]

When used to monitor internal traffic, traditional perimeter firewalls limit scalability because they force the traffic to be hair-pinned through a centralized appliance. In addition to causing performance bottlenecks and latency issues, traditional firewalls create further complexity because they don't easily support the creation and management of security groups for network segmentation. Implementing policies such as those needed to secure complex, modern applications can require thousands of rules using a traditional firewall.

To simplify operations while scaling seamlessly and cost effectively as they support change and growth in the distributed application environment, security operations teams need an internal firewall that can:

- Support virtual security zones (network segments) without enormous cost and constraint on traffic volume and policies.
- Automatically manage security policies across the lifecycle of thousands of hosts and workloads.
- Reduce capital expenditures by replacing multiple discrete appliances.

Customer experience: Replacing hundreds of appliances

To protect a business-critical, consumer-facing mobile application, a global telecommunications company with 400 million users in more than a dozen countries needed to segment and secure large amounts of network traffic on its in-house infrastructure. The company's hardware-based firewall could not scale to protect all workloads and traffic across dev/test, production and demilitarized zones.

Because the traffic was hair-pinned to and from the firewall appliances, the company experienced performance issues during traffic spikes when new versions of the application were released. The traditional firewall also did not have enough capacity in its rule tables to support all the rules required to protect the application's complex back-end infrastructure.

The telecommunications company is replacing more than 200 firewall appliances with the VMware Distributed Firewall, giving it a single firewall model and management console for the entire infrastructure. VMware simplifies operations for the company and eliminates performance bottlenecks. Within the Distributed Firewall, security tags simplify management of firewall rules by allowing policies to be expressed using tags rather than an IP address. This gives the company greater agility and speed for adding new workloads, and moving or decommissioning existing ones.

[2] VMware. Internal projection based on analysis of 192 customer ROI models using the Data Integrated Customer Engagement (DICE) business case tool. January 2020.

Conclusion

Savvy CISOs across many industries have already discovered they can dramatically reduce cost and complexity, and improve scalability, when securing internal workloads and traffic by implementing an internal firewall. Instead of relying on traditional, bolted-on security solutions, these organizations turn to intrinsic security—built in, distributed and application-aware—to protect the brand.

With the VMware Distributed Firewall, companies gain a distributed, scale-out internal firewall that protects all east-west traffic to mitigate risk and enable compliance. By reinventing the internal firewall deployment model, the Distributed Firewall simplifies operations with security that's intrinsic to the infrastructure.