White Paper: **May 2022**

Protecting Physical Workloads in the Private Cloud

vmware®

Table of contents

Workloads that only run on physical servers

Most enterprise workloads today are virtualized, but not all workloads can be. In particular, workloads must run on physical servers if they have:

- High or specific hardware-dependent performance requirements; high-performance computing (HPC) workloads are the primary example of this sort of workload
- Been designed to run only on legacy operating systems; this includes mainframe applications and databases
- Device-specific system requirements, such as the unusual memory, power consumption, and processing needs of operational technology (OT) systems and medical devices
- The need to conform to specific security or policy requirements that stipulate that they cannot be virtualized

Introduction

Over the past year, pandemic-related uncertainties, the rise of remote work, and a surge in ransomware attacks have added to security professionals' challenges. Given the extent of the demands faced by security teams, the need to secure organizational networks in ways that are consistent, comprehensive, and easy to administer is greater than ever. Networks must be appropriately architected and segmented to prevent lateral movement by attackers, robust threat detection capabilities must be in place, compliance must be maintained, security policies must be enforced, and access to on-premises and cloud-hosted resources must be securely enabled. All without placing an undue burden on security practitioners.

Enterprises can make great strides towards achieving these objectives by applying the right firewalling strategy. This will involve a combination of internal and edge firewalls. Internal firewalls are important because they protect communication between workloads within the enterprise environment (this communication comprises the vast majority of network traffic, and monitoring it is essential for blocking lateral movement). Because most workloads in the private cloud (or modern data center) are virtualized, a solution like the VMware NSX Distributed Firewall is ideal for inspecting and protecting the traffic that travels between them.

However, there are often a few (and sometimes more than a few) physical workloads in most data centers. These are workloads that run directly on an operating system without an intermediate hypervisor. To ensure that there's complete protection of all workloads in the private cloud—both physical and virtualized—security teams need to secure all east-west traffic, which includes traffic going to or coming from these physical workloads as well as virtualized ones.

Deploying a solution like the VMware NSX Gateway Firewall in conjunction with the NSX Distributed Firewall makes it possible to extend the same unified, consistent access control and threat protection capabilities that the NSX Distributed Firewall supplies across all workloads in the private cloud. And this comprehensive protection can be achieved within a single management console and software-only solution portfolio. This reduces the administrative burden that security teams face while empowering them to deliver consistent protection everywhere. This way, defense-in-depth can be achieved at the boundaries of all workloads—whether they're virtual, physical, or containerized—with ease and efficiency.

Firewall solutions for securing physical workloads

To defend against today's threat actors, who are constantly advancing their capabilities and sophistication and working tirelessly to seek out the single weakest point in any environment, organizations need to enforce all security policies with absolute consistency. This should be the case regardless of whether your workloads are running on virtual machines (VMs), in containers, in the cloud, on physical servers—or any combination of the above. Providing seamless and consistent policy enforcement for physical workloads in a private cloud poses unique challenges, however.

It's always a best practice to isolate network defenses from endpoint defenses whenever possible. This increases the overall resilience of the security architecture: should network defense mechanisms be compromised, the security team can still fall back upon endpoint-based systems to contain the attackers, or vice-versa. But it's also preferable to deploy as few defense systems as possible to limit the overall complexity of the security environment and improve manageability. For this reason, security teams prefer to deploy network security solutions that are independent of operating system (OS) provided firewalls.

With that said, three strategies can be followed to integrate physical workloads into the VMware NSX Data Center environment. These are:

1. Installing an agent on the physical server

Agents can be installed on physical servers running certain OSs, though this sometimes requires additional OS features or modules. Once the agent has been installed, it can enforce NSX policies and be managed within the NSX Distributed Firewall console.

This approach doesn't require additional physical switches or hardware and isn't subject to capacity limitations associated with such hardware. It also brings all the benefits inherent to the software-defined approach to firewalling, including the fact that features can be deployed as soon as new capabilities are developed and released.

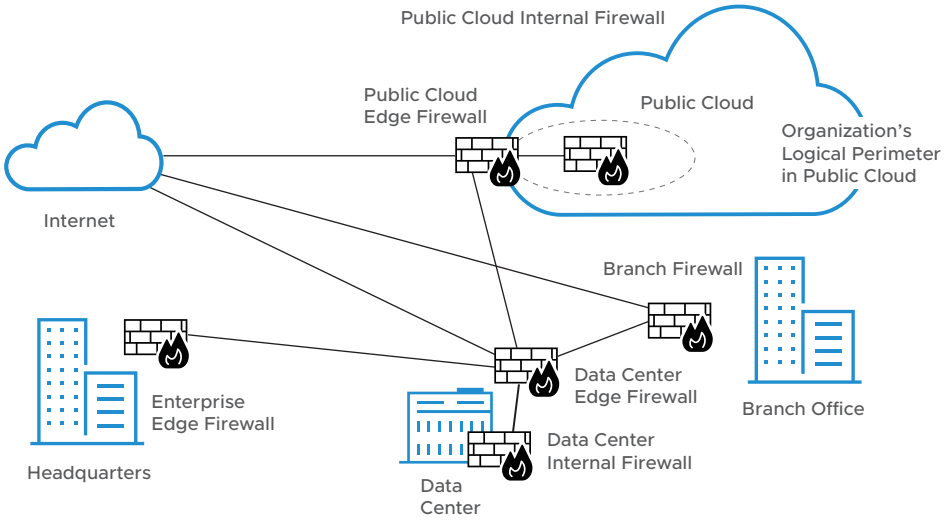
However, agents are available only for some server OSs. Further, an agent represents another piece of software to run on a physical server that may already be overloaded with services and agents. This may increase security teams' workload, when installing, configuring, and managing the agents.

2. Enforcing policies on virtual workloads

It isn't always necessary to install an agent or other software directly onto the physical server whose workloads you'd like to secure within NSX. This is because it's possible to extend NSX's security benefits to any workload that communicates with a virtualized workload by configuring firewalling policies at the virtualized workload.

This enables security teams to apply policies consistently, regardless of workloads' location or type, with no need to rely on or manage the physical server's native OS capabilities. In this way, this approach can simplify and unify the overall security experience.

However, the approach described above can only be used to protect workloads that communicate with virtualized workloads, and as a result, cannot protect physical server-to-physical server traffic. If you need to protect traffic traveling between physical servers, this approach will not be adequate or require an additional solution that will nullify its simplicity benefits.



3. Deploying the NSX Gateway Firewall at the boundary of physical workloads

The NSX Gateway Firewall can filter traffic in a stateful or stateless manner, includes enhanced security functionalities, and provides traffic flow management capabilities. This makes it ideal for protecting physical workloads in the private cloud, where it doesn't require access to the OS or hypervisor.

The NSX Gateway Firewall can also serve as a Private Cloud zone firewall (a firewall at the data center perimeter, between the edge and the internal firewalls) or a Public Cloud edge firewall (see figure).

By deploying the NSX Gateway Firewall, it's possible to protect workloads of all types, extending the security coverage of the NSX Distributed Firewall without introducing additional administrative complexity since both the NSX Distributed Firewall and the NSX Gateway Firewall are managed together with the same dashboard.

Features and benefits of the VMware NSX Gateway Firewall

The NSX Gateway Firewall has all the traditional layer 2-7 firewall capabilities. Further, it brings all the inherent advantages of a software-defined firewalling strategy, including consistency, operational simplicity, and cost-effectiveness.

Long deployed to protect physical workloads in the private cloud, the NSX Gateway Firewall received a set of architectural enhancements in VMware NSX 3.2.1 that have expanded its capabilities—and increased the number of use cases for which it's appropriate. The NSX Gateway Firewall not only incorporates a robust set of networking features but is also optimally suited to provide secure connectivity, access control, and threat prevention.

User identity-based access controls

Robust user identity-based access controls to ensure that people access the applications and resources they need to get their jobs done and only those applications and resources. These controls also mitigate the risk of insider threats.

Application-based access controls

Automatically identifying workloads and enabling security teams to create security policies based on workload type can simplify policy formulation and maintenance.

Other access controls

The NSX Gateway Firewall offers URL filtering and network address translation (NAT) to exclude communication with known malicious sites.

Advanced threat prevention capabilities

The NSX Gateway Firewall incorporates a full complement of threat detection and prevention capabilities, including intrusion detection/prevention (IDS/IPS), malware detection via network sandboxing, and full Transport Layer Security (TLS) decryption. This enables it to identify and automatically block today's most pressing threats.

High capacity, high availability

With support for active-active stateful high availability for up to eight nodes, the NSX Gateway Firewall has more high-capacity attributes than a traditional software-based firewall, which couldn't extend its capacity beyond what two physical servers could support.

A highly capable partner to the NSX Distributed Firewall

Because it was purposefully designed to complement the NSX Distributed Firewall, the NSX Gateway Firewall shares many operational constructs and has a common management console. This greatly simplifies the combined management of the NSX firewall suite. When the NSX Distributed Firewall is paired with the NSX Gateway Firewall, it's possible to extend their access control and advanced threat prevention capabilities across the entire private cloud environment, protecting physical and virtualized workloads alike.

Together, the NSX Distributed Firewall and the NSX Gateway Firewall can handle all east-west traffic in the private cloud. This includes virtual-to-virtual communications along with virtual-to-physical, physical-to-virtual, and physical-to-physical. What's more, they can provide consistent network security coverage to this diverse set of dynamic workloads while facilitating operational simplicity, a win-win for security teams.

Why add the NSX Gateway Firewall to an NSX Distributed Firewall Deployment?

The NSX Gateway Firewall seamlessly extends the Distributed Firewall's protection across all physical workloads in a private cloud. It can also serve broader firewalling needs in the data center if this makes sense within your network security architecture.

With the full VMware NSX firewall suite, you can:

- **Extend consistent network security coverage across the whole of the infrastructure.**
  When used alongside the NSX Distributed, the NSX Gateway Firewall makes it simple to enforce consistent policies for all private and public cloud workloads. And this can be done with a software-only strategy so that there are no specialized hardware appliances to purchase, deploy or manage on an ongoing basis.
- **Unify management across the NSX Gateway Firewall and the NSX Distributed Firewall.**
  All of your organization's firewall management needs can be met within one centralized, user-friendly management console.
- **Reduce costs.**
  Because there's no need to purchase specialized hardware, you'll lower your organization's capital and operational expenditures both. Not only will you avoid the cost of appliances and associated management contracts, but you'll also save due to reduced management overhead. With a simpler deployment that provides consistent network security coverage with unified management, security teams can work smarter, not harder, while achieving superior protection for all workloads in the private cloud.

Enjoy deployment flexibility

It's possible to run the Gateway Firewall directly on a physical server or as a virtual form factor. This flexibility means that it can be implemented in the way that best suits your organization's security and management needs. It also enables your security team to deploy the option with the best performance for the organization's unique set of workloads.

There are modest performance gains from running the NSX Gateway Firewall directly on the physical server (as an ISO image). Selecting this deployment option can also reduce administrative overhead. In other cases, a virtual form factor is more desirable. Regardless, the NSX Gateway Firewall will provide expansive firewalling capabilities with no need for specialized hardware.

Conclusion

To counter today's sophisticated security threats without placing an undue burden on security teams, organizations must focus on solutions that enable them to extend consistent and unified protection to all workloads in the private cloud, regardless of whether they're physical or virtual. It's essential to choose a security and firewall portfolio that meets compliance and security policy needs while remaining easy to administer, even as the environment changes or scales up.

A software-defined solution purpose-built to complement the VMware NSX Distributed Firewall, the VMware NSX Gateway Firewall enables the Distributed Firewall's capabilities to be seamlessly extended to physical workloads in the private cloud. Without increasing management overhead or costs, the VMware NSX firewall portfolio offers consistent protection for every user, application, and workload in your environment – including those relying on containers or the public cloud. Pairing the NSX Distributed Firewall with the NSX Gateway Firewall is an effective strategy for mitigating risk while ensuring operational simplicity so that even the most resource-constrained security teams can get more done in less time.

Item No: vmw-wp-protecting-physical-workloads-uslet-v5 5/22