VMware NSX Gateway Firewall

Extend unified, consistent protection across the entire enterprise environment

At a glance

VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that enables you to achieve consistent network security coverage and unified management for all of your workloads, regardless of whether they're running on physical servers, in a private or public cloud environment or in containers. When deployed together with the NSX Distributed Firewall, the Gateway Firewall extends its capabilities to deliver consistent protection across the entirety of the infrastructure.

Key benefits

- **Enforce consistent policies everywhere:** When the NSX Gateway Firewall is deployed in conjunction with the NSX Distributed Firewall, it's easy to extend consistent layer 2-7 security controls across all applications and workloads, whether they're running in the private or public cloud. This ensures that all workloads everywhere are subject to the same security policies.
- **Unified management:** The NSX Gateway Firewall shares the same management console as the NSX Distributed Firewall. This makes it simple to enforce consistent policies at the perimeter, between zones and inside the organizational network.

Part of a comprehensive private cloud firewall portfolio

As hybrid becomes the cloud strategy of choice for a growing number of enterprises, it's increasingly important to standardize architectures and maintain uniform, consistent security policies everywhere. The VMware NSX Gateway Firewall makes it possible to extend the advanced threat prevention capabilities of the VMware NSX Distributed Firewall to physical workloads in the private cloud and provide defense-in-depth at the boundaries of sensitive security zones, no matter where they're located or whether they're virtual, physical or containerized.

A firewall to meet today's needs

VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), URL filtering and malware detection (using network sandboxing and other techniques) as well as routing and virtual private networking (VPN) functionality.

Key capabilities

Networking capabilities
The NSX Gateway Firewall provides a full suite of static and dynamic routing capabilities including IPv4 and IPv6, DNS, DHCP and comprehensive IP address management (IPAM).

Secure connectivity services
With support for layer 2 and 3 VPN services, the NSX Gateway Firewall enables secure low-latency connectivity across geographically diverse sites.

Access control
The NSX Gateway Firewall supports consistent enforcement of layer 2-7 access policies including application identity and user identity-based controls, URL filtering and network address translation (NAT).

Key benefits cont'd

- **Cost savings:** Because the NSX Gateway Firewall runs on readily available server hardware, there's no need to purchase specialized hardware appliances or associated management contracts. You'll experience additional savings on operational expenditures due to the Gateway's Firewall's simplicity of management.

Learn More

Check out these resources to learn more about protecting your entire ecosystem with a comprehensive, unified firewall solution. Reach out to your VMware Sales Representative for further details.

- Read about the VMware NSX Gateway Firewall
- Learn more about the VMware NSX Distributed Firewall

Threat control

The NSX Gateway Firewall incorporates advanced threat prevention capabilities to identify threats and block attacks. These include IDS/IPS, malware detection that's integrated with network sandboxing, and full Transport Layer Security (TLS) decryption.

Platform capabilities

The NSX Gateway Firewall includes platform capabilities such as active-standby for high availability and native support for multi-tenancy to easily operationalize multi-tenant deployments.

Deployment flexibility

The NSX Gateway Firewall is available in two form factors: a virtual machine or an ISO image that can run on a physical server with no intermediary hypervisor. In either case, it can expand your firewalling capacity with no need for specialized hardware.

Features	NSX Gateway Firewall	NSX Gateway Firewall with threat prevention	NSX Gateway Firewall with advanced threat prevention
L2-L4 access control	X	X	X
Static, dynamic routing	X	X	X
L2 and L3 VPNs	X	X	X
User identity-based access control	X	X	X
Application identity-based access control	X	X	X
URL filtering	X	X	X
TLS decryption	X	X	X
IDS/IPS		X	X
Network sandboxing			X

Use cases

- **Protect physical workloads in the private cloud:** Extend the same security policies across all of your workloads, no matter where they're running, with no need to purchase or manage separate appliances.
- **Private cloud zone firewall:** Unify north-south and east-west security with stateful firewalling between multiple zones across the organizational environment.
- **Public cloud edge firewall:** Enforce consistent policies with advanced threat prevention that extends right up to the public cloud edge.

Firewall performance and resource requirements

The table below summarizes the performance characteristics of the NSX Gateway Firewall under different resource envelopes.

Form Factor	Large (8 vCPU, 16GB RAM)	X-Large (16 vCPU, 64GB RAM
Firewall throughput (64 KB HTTP)	20 Gbps	24 Gbps
IPsec VPN throughput	13 Gbps	21 Gbps
IDS/IPS (64 KB HTTP)	1.5 Gbps	4.5 Gbps
Malware detection (64 KB HTTP)	Not supported	3.5 Gbps
New sessions per second	306 K	310 K
Max sessions	2.1 million	4.2 million

The performance results shown above were tested under the following conditions:

- Firewall and IPsec VPN throughput measured with Intel® Xeon® CPU E5-2660 v4 2.00GHz with 40G port network interface card.
- Firewall throughput measured with 64 KB HTTP transactions.
- IPsec VPN throughput measured with AES-128 GCM encryption and 1462-byte packets.
- IDS/IPS tested with an inspection depth of 8KB

A capable partner to the NSX Distributed Firewall

Disparate security solution sets introduce management complexity, increasing costs and risks along the way. The VMware NSX Gateway Firewall was purpose-built to extend the capabilities of the VMware NSX Distributed Firewall across all workloads in your organization, including those running on physical servers. With a tightly integrated firewall portfolio, security teams can accelerate operations and effectively mitigate risk, without increasing costs.