SOLUTION BRIEF

Fortinet Delivers Automated, Advanced Security for VMware NSX-T Data Center Environments

Executive Summary

VMware NSX-T Data Center addresses the evolving needs of organizations to support cloud-native applications, bare metal workloads, multi-hypervisor environments, and multiple public clouds. NSX-T Data Center is expected to be widely adopted in the coming year.

While NSX-T provides basic firewall capabilities, organizations facing expanding digital attack surfaces need more. FortiGate VM for NSX-T augments VMware security with robust protection for both east-west and north-south traffic. A virtual appliance that integrates with NSX-T Data Center through service insertion as a third-party edge firewall, FortiGate VM performs next-generation firewalling (NGFW), inspection of encrypted secure sockets layer (SSL)/transport layer security (TLS) traffic, intrusion prevention (IPS), and web application control. Fortinet is one of the first security vendors that delivers complete integration with the NSX-T Data Center 2.4, 2.5, 3.0 and 3.1 releases.

Why NSX-T Customers Need Advanced Security

To address an expanding digital attack surface, security architects need to evolve their security infrastructure to effectively manage risks across software-defined data centers (SDDC) as well as in private and public clouds.

The evolving security infrastructure will need to contend with a variety of adverse conditions. As more than 72% of internet traffic is now encrypted,[1] there is an increasing risk of malware hiding in encrypted traffic between the virtualized data centers and various clouds. In fact, 60% of malware uses encryption to avoid detection.[2] There is also the risk of lateral movement of threats within virtualized data centers and across the clouds, which can speed attacks and increase the scale of impact. These conditions and others point to the need for advanced (L7) security solutions that can perform and scale at the pace of multi-cloud and hybrid cloud deployments.

Key Benefits:

- Advanced (L7) threat protection integrated with VMware NSX-T Data Center environments in SDDCs as well as private and public clouds
- Zero-trust segmentation to protect against lateral threats
- High-performance throughput powered by virtual SPU technology in FortiGate
- Streamlined SecOps, with automation and orchestration via Fortinet Fabric Connectors
- Broadest public cloud coverage, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud, and Alibaba Cloud
- Single-pane-of-glass management through VMware NSX Manager, with full visibility in FortiManager

What FortiGate VM Adds to VMware NSX-T Data Center

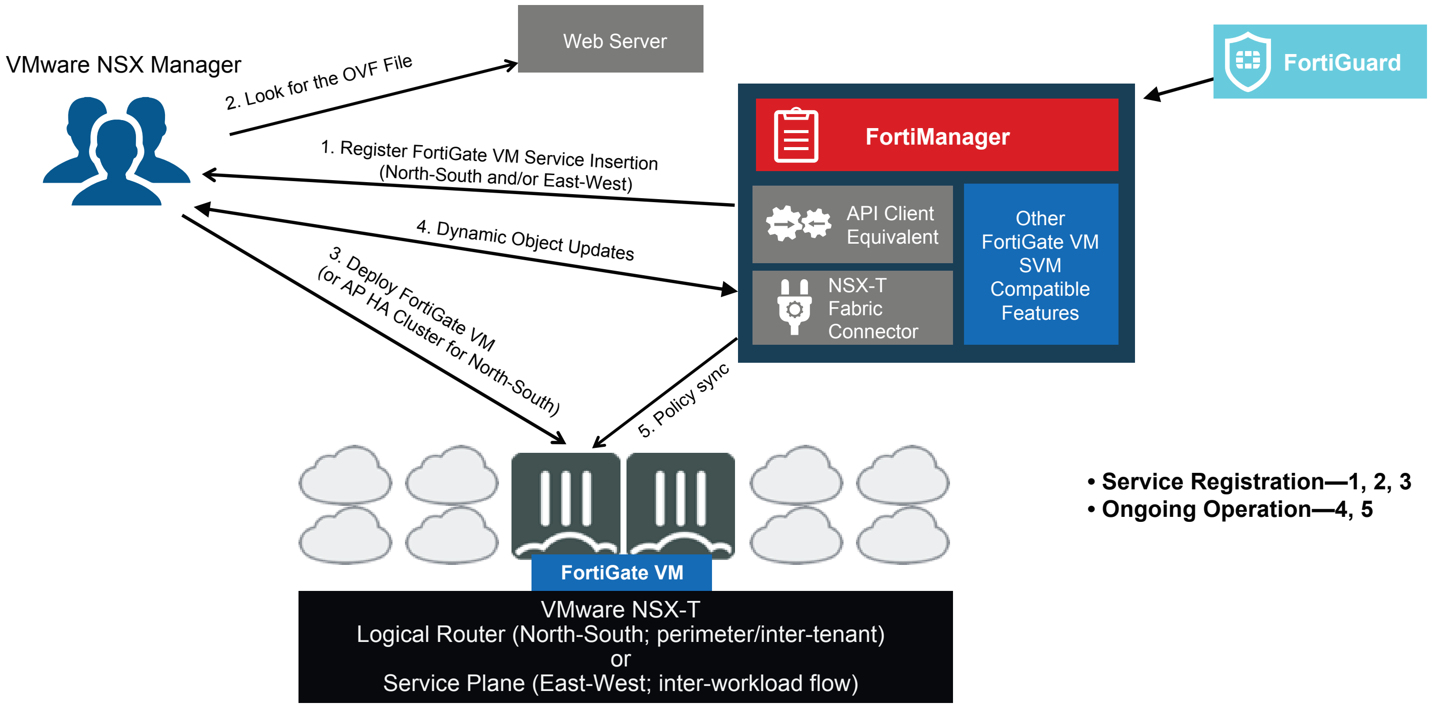
FortiGate VM NGFW is a virtual appliance that integrates with NSX-T security for VMware ESXi and other hypervisors and container orchestration platforms in SDDCs, private clouds, and public clouds. FortiGate VM augments the microsegmentation provided by NSX-T 2.4 with advanced L7 security and zero-trust segmentation for complete protection against the most sophisticated threats and vulnerabilities.

How FortiGate VM Works in NSX-T SDDCs and Cloud Environments

The FortiGate VM provides interoperability with NSX-T Data Center through service insertion as a third-party edge firewall (Figure 1). Core capabilities include:

- By means of Fabric Connectors activated from the FortiManager console, FortiGate VM integrates with NSX-T Data Center to register both east-west and north-south service insertions.
- From that point on, security can be managed from the NSX-T dashboard and is automatically carried through to the FortiGate VM instances running in the NSX-T Data Center.

- Fortinet Fabric Connector automatically updates security policies associated with dynamic objects in NSX-T whenever changes are made to underlying IP addresses, application metadata, and annotations. This capability, which also extends to public cloud infrastructures (such as AWS, Azure, and GCP), relieves organizations of the need to manually update security policies, freeing up their time for other business-critical duties.


VMware NSX Manager
Web Server
FortiGuard
FortiManager
API Client Equivalent
NSX-T Fabric Connector
Other FortiGate VM SVM Compatible Features
2. Look for the OVF File
1. Register FortiGate VM Service Insertion (North-South and/or East-West)
4. Dynamic Object Updates
3. Deploy FortiGate VM (or AP HA Cluster for North-South)
5. Policy sync
FortiGate VM
VMware NSX-T
Logical Router (North-South; perimeter/inter-tenant)
or
Service Plane (East-West; inter-workload flow)

- **Service Registration—1, 2, 3**
- **Ongoing Operation—4, 5**

Figure 1: FortiGate VM and FortiManager seamlessly integrate with VMware NSX Manager.

Unique Advantages of Fortinet

- **Scalable east-west and north-south security.** Featuring FortiGate VM virtual SPU (vSPU) technology and parallel-path architecture, FortiGate is the industry's highest-performing virtual NGFW. These features enable it to perform SSL/TLS inspection, in addition to its other threat protection tasks, with the least impact on throughput and with the lowest total cost of ownership (TCO) per protected Mbps.[3] This allows NSX-T users to simultaneously optimize both north-south and east-west security while maintaining network service-level agreements (SLAs).
- **Zero-trust segmentation.** Aware of the dangers of implicit, static trust in flat internal networks, security architects are adopting zero-trust strategies. FortiGate VM for NSX-T virtual cloud network implements zero-trust segmentation, with trust levels continually updated through multiple trust verification sources. This reduces the risk that a threat that has penetrated the edge firewalls will move freely throughout the SDDC or cloud environment.
- **Streamlined SecOps.** As a Fabric-Ready Partner, VMware enables Fortinet to natively integrate with its products and solutions, offering a range of benefits for SecOps teams:
  - Automated updates to NSX-T dynamic objects and firewall policies through the **FortiGate Fabric Connector for NSX-T** reduce operational overhead and streamline application life-cycle management.
  - Single-pane-of-glass management minimizes staff training and helps lean IT and security teams achieve both their network SLAs and their security objectives.
  - Automation and orchestration with Fabric-Ready Partners minimize integration work and enable IT and security teams to leverage existing investments.

Not Just a Virtual Firewall, Also a Complete Security Fabric

FortiGate VM is part of the Fortinet Security Fabric. This unique network security architecture offers a broad, integrated, and automated approach to detecting and responding to the full range of threats to SDDCs, private and public clouds, and the workloads and data they support.

In addition to FortiGate and FortiManager, there are several other key Security Fabric components of interest to VMware NSX-T users:

FortiOS. Powering the entire Fortinet Security Fabric, FortiOS allows organizations to achieve a security-driven network with one intuitive operating system.

FortiGuard threat intelligence services. A continual global threat-intelligence feed from FortiGuard Labs keeps all Security Fabric components up to date in real time.

FortiAnalyzer. Analytics and log management enables organizations to achieve deeper insights into advanced threats by detecting and correlating threat-intelligence, automating workflows and compliance reporting, and orchestrating log management.

FortiSandbox. This sandboxing solution quarantines and inspects suspicious packets to contain zero-day threats before they impact the business. By sharing new threat information through FortiGuard Labs, FortiSandbox helps contribute to the identification of previously unknown threats for the benefit of the entire security community.

FortiDeceptor. This threat-deception solution automates the creation of decoys and deceptive VM instances to deceive internal and external threats and subsequently expose threat sources and eliminate threat impacts by breaking the kill chain.

Partnership Pays Off for NSX-T Customers

While VMware continues to define the leading edge of virtual network connectivity, Fortinet supplies industry-leading artificial intelligence (AI)-driven security for NSX-T Data Center environments. The strong partnership between Fortinet and VMware gives customers additional confidence to expand their investments in the Virtual Cloud Network.

[1] John Maddison, "More Encrypted Traffic Than Ever," Fortinet Blog, December 10, 2018.

[2] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[3] Thomas Skybakmoen, "Next Generation Firewall Comparative Report: Security Value Map™ (SVM)," NSS Labs, July 17, 2018.