SOLUTION BRIEF

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

Executive Summary

VMware NSX-T, a stand-alone software-defined networking (SDN) platform, addresses the use cases that NSX-V does not support. NSX-T is expected to be widely adopted in the coming year as enterprises increasingly use multiple hypervisors, containers, and multiple clouds.

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.

Cloud Adoption Expands Attack Surface

Rapid cloud adoption means a rapidly expanded attack surface. A recent survey predicts that 83% of enterprise workloads will be in the cloud by 2020.[1] Further, based on recent research, the average enterprise uses as many as 91 different cloud applications.[2] Most of these are adopting multi-cloud approaches, which result in security silos that obfuscate security visibility and make it difficult to manage them through centralized controls.

Clearly, there is no shortage of attack vectors. Cloud workloads and applications, whether in the public or private cloud, or Software-as-a-Service (SaaS), must be protected from sophisticated threats with reliable, elastic security.[3]

Encrypted Traffic at a Record High

As more and more data is migrated from on-premises data centers to the cloud, this dramatically expands the amount of encrypted traffic traversing the internet. One study finds that more than 72% of internet traffic is now encrypted.[4]

While encrypted traffic protects data from bad actors, it is not without its risks. Cyber criminals are increasingly using it to deliver malware into their intended targets. Unless this encrypted traffic is inspected with the right security tools, an organization can suddenly find itself facing a potential data breach or operational disruption. But many next-generation firewall (NGFW) solutions either lack secure sockets layer (SSL)/transport layer security (TLS) inspection capabilities or the performance to conduct inspections without adding more NGFWs—and thus cost.

Joint Solution Components

- Fortinet FortiGate
- VMWare NSX-T

Top Features:

- Advanced threat prevention for VMware NSX-T SDDC environments
- Automated deployment and orchestration of FortiGate VM for SDDCs and private and public clouds
- Single-pane-of-glass management and full visibility with FortiManager
- Seamless security scaling from SDDCs to private and public clouds
- Inspection of encrypted traffic without impacting network performance

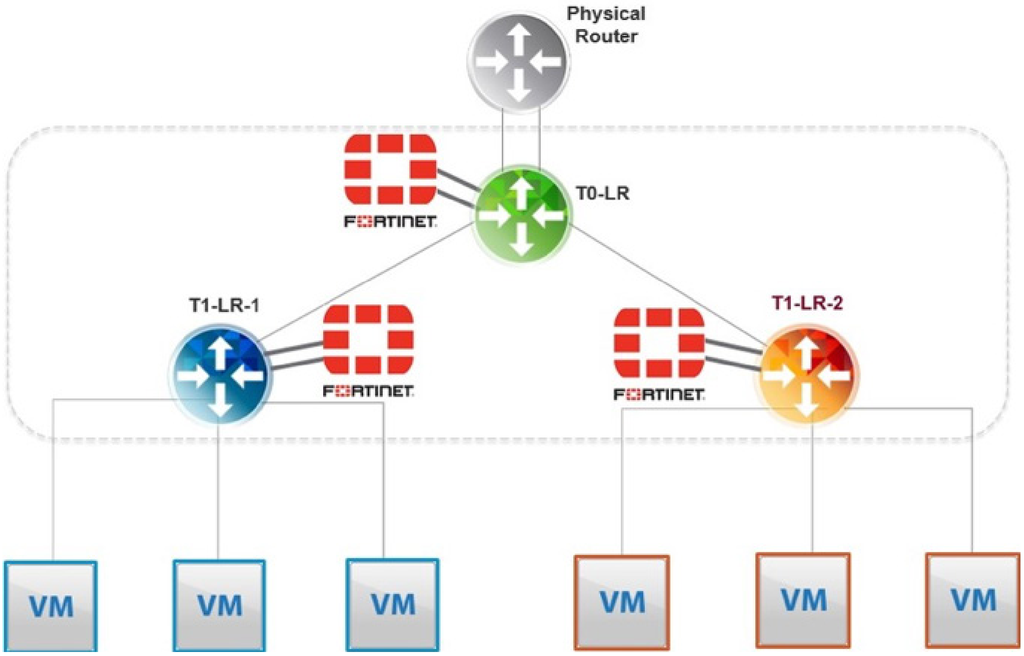
vmware READY NETWORKING AND SECURITY

Fortinet Support for NSX-T Data Center

NSX-T connects all types of applications and is multi-hypervisor aware. It is an SDN stack that supports hypervisors beyond vSphere, such as KVM and OpenStack. In addition, it supports container platforms such as Kubernetes and Docker.

The FortiGate VM next-generation firewall (NGFW) integrates with NSX-T to provide security for hypervisors and container orchestration platforms. This results in seamless and consistent security for the applications running on these platforms. It provides purpose-built integration for VMware's software-defined data center (SDDC) and interoperability with NSX-T through service insertion as a third-party edge firewall.

FortiGate VM also protects the north-south (vertical) traffic flow inside the NSX-T environment. It does so, as depicted in the diagram below, by integrating with logical routers in tier 0 and/or 1, depending on where to inspect the traffic. NSX-T connects workloads running in SDDCs and public and private clouds. FortiGate VM enforces security at the connection points between these disparate networks.



Fortinet Advantages

The Fortinet Security Fabric delivers a more comprehensive and faster response to threats, while enabling organizations to realize improved efficiencies. Specific operational advantages include:

- Automatic identification and containment of threats in real time
- Seamless security scaling from data centers to clouds
- Compatibility with new versions of VMware on AWS
- Smooth failover with active/passive high availability (HA)
- Improved efficiency with single-pane-of-glass management and visibility with FortiManager
- Ability to examine encrypted traffic with no network slowdown

The Security Fabric also offers threat-intelligence advantages that include:

- Integrated, comprehensive security posture across the network with sandbox and content security integration via the Fortinet Security Fabric
- The latest threat intelligence delivered in near real time by FortiGuard Labs
- Efficient, top-rated protection for disparate multi-cloud environments

The Best Way to Secure NSX-T Environments

If you are running NSX-T, you need dynamic security that can enforce security policy across multi-hypervisor and container environments. FortiGate VM integration with VMware's NSX-T solution extends the NSX-T firewall functionality with advanced security services and allows enterprises to reap all the benefits of SDDCs and public and private clouds with agility and efficiency.

Advanced Layer 7 security with FortiGate VM for traffic moving between virtual machines and external networks secures customer assets and data in the cloud against even the most sophisticated threats. FortiGate VM includes multi-layered protections such as firewall, application control, IPS, sandboxing, and threat-protection technologies.

[1] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

[2] Scott Brinker, "The average enterprise uses 91 marketing cloud services," Chief Marketing Technologist Blog, June 12, 2017.

[3] "Quarterly Threat Landscape Report Q3 2018," Fortinet, November 2018.

[3] John Maddison, "More Encrypted Traffic," Fortinet Blog, December 10, 2018.

June 23, 2021 10:07 AM

366164-A-0-EN