

**SOLUTION BRIEF**

# Simplifying security for any app at any scale on hybrid cloud and multi-cloud deployments

## Securing Virtual Networks with Nutanix Flow and FortiGate-VM

### The Challenge

Organizations of various sizes have cloud adoption at the center of their Digital transformation strategy. The movement of applications to hybrid cloud and multi-cloud brings immense benefits but increases the cyberattack surface. They face a double-edged sword with a tightening regulatory environment and rapidly worsening cyber threat landscape. Costs of penalties are high and risk to brand reputation is even higher. There is a critical need to identify, inspect, visualize and secure ingress and egress application traffic flows across hybrid cloud and multi-cloud networks.

### The Joint Solution

Fortinet and Nutanix form a software-defined solution with secure, scalable, hyperconverged infrastructure for virtualized applications. The FortiGate-VM running on Nutanix AHV provides deeper visibility into applications and prevents known and Zero-day cyber threats, while Nutanix enables you to meet the growing demands of enterprise applications, hybrid-cloud, and multi-cloud environments.

FortiGate-VM enables hybrid cloud and multi-cloud traffic to be segmented based on the application and then inspected for known and Zero-day threats such as C&C, malware, ransomware etc. Policy based redirection from Flow™ gives NetOps and SecOps teams granular control over traffic inspection and optimizes resource consumption. Automation features and centralized management enable you to ensure that security policies can keep pace with any contextual changes in your enterprise cloud environment.

Nutanix and Fortinet have validated two modes for deployment flexibility. Choose layer 3 routed mode for FortiGate-VM on Nutanix AHV to inspect traffic while acting as a layer 3 gateway. Use layer 2 vWire mode as part of Nutanix Flow traffic redirection to transparently direct VM traffic through a FortiGate-VM firewall running on every AHV host.

- L7/ DPI / Advanced Security with FortiGate-VM
- Cluster wide deployment of service chains with Nutanix Calm
- Multiple Services Per Chain
- Policy Based Selective Traffic Redirection

### Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall, FortiManager, FortiAnalyzer, FortiADC, FortiMail, FortiSandbox, FortiSIEM, FortiAuthenticator, FortiNAC, FortiProxy

### Joint Solution Benefits

- Segment and control East-West VM traffic
- Advanced L7 security protection and automated remediation
- Add policy based Deep Packet Inspection (DPI) between virtual machines (VMs)
- Identify and control traffic flowing into your secure environment; limit application access based on users and groups; block known and unknown threats
- Securely deploy applications faster and scale at the pace of modern business
- Predictable scale-out architecture to seamlessly expand desktop and server virtualization pilots to full production deployment



## Diagram of Joint Solution

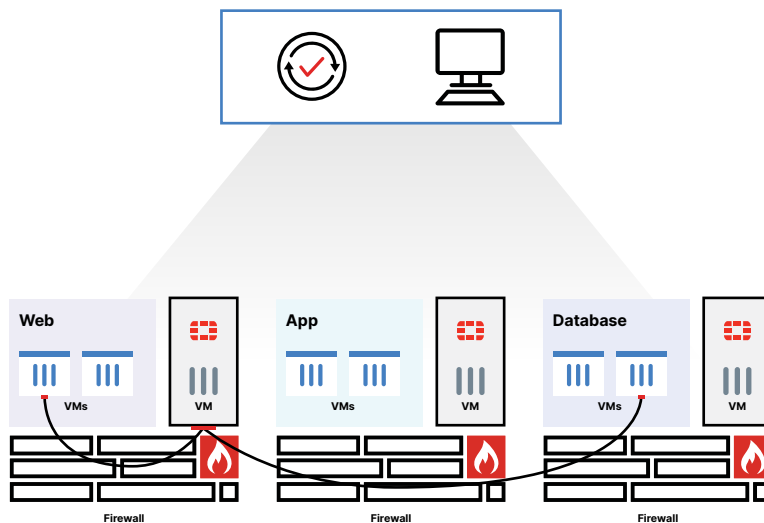


Figure 1: Service chaining Nutanix deployments with Nutanix Flow™ and FortiGate VM.

## Solution Components

### Fortinet Security Fabric

The Security Fabric allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between Internet of Things (IoT), devices, and cloud environments throughout the network.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.

### Fortinet FortiGate VM Next-generation Firewall

Your virtualized data center assets need advanced protection from evolving threats, both known and unknown.

FortiGate VM is a virtualized form factor of our market leading, high performance FortiGate next-generation firewall (NGFW) that delivers advanced security protection for north-south and east-west traffic in software-defined data centers and cloud. Based on the powerful FortiOS operating system and FortiGuard Threat Intelligence services, FortiGate virtual NGFW delivers industry-leading performance and layered threat protection of your software-defined data center traffic, with a single pane-of-glass to manage your physical and virtual network.

### Nutanix Flow Networking

Nutanix Flow™ is a software-defined network (SDN) policy engine built into AHV virtualization, with nothing to install and no requirements to alter or reconfigure your physical networking. Flow™ provides VM level application microsegmentation, virtual network segmentation, and policy-based network service insertion.

Flow makes it easy to visualize and discover VM communications and create policy for all virtualized network traffic.

Using service insertion, Flow enables policy-based VM traffic redirection through FortiGate VM firewalls, expanding visibility and control.

## About Nutanix

Nutanix, the leader in hypervconverged infrastructure (HCI), makes datacenter infrastructure and clouds invisible, elevating IT to focus on business applications and services. Its Enterprise Cloud OS software converges private, public and distributed clouds, bringing one-click simplicity and agility to infrastructure and application management. This enables IT to rapidly deliver against business needs at a favorable TCO, while retaining hardware and virtualization technology that best suit their skills.

Learn more at [www.nutanix.com](http://www.nutanix.com).



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.