Fortinet Private Cloud Security Solutions

Use Cases for Comprehensive Protection

Table of Contents

Executive Overview

Organizations are embracing private cloud deployments as a way to save cost and increase control of key corporate resources. Many elect to deploy private clouds to keep their most sensitive data on-premises while maintaining other services in public clouds—a hybrid cloud model. Organizations that invest in hybrid cloud infrastructures often realize significant business value through increased efficiency, reduced costs, and an improved risk posture. However, like almost any computing infrastructure, private clouds bring their own unique security challenges.

Fortinet is a leading multi-cloud security provider and provides a robust private cloud security solution based on FortiGate-VM virtual next-generation firewalls (NGFWs). The Fortinet solution enables centralized monitoring and control of internal and external network traffic and helps organizations get on top of compliance challenges. The FortiGate NGFW and a wide array of supporting solutions are available in virtual machine (VM) form factors with all the features and functionality of physical appliances, a good fit for a highly virtualized private cloud. The solution integrates seamlessly with the Fortinet Security Fabric, providing transparent visibility, centralized control, and full automation of security processes.

Introduction: Private Clouds Present Their Own Security Challenges

Organizations of all sizes have moved to the cloud,[1] but the role of private clouds in that trend is often downplayed. One study shows private clouds now growing more quickly than public ones,[2] and the private cloud services market is projected to grow by 21% annually between now and 2023.[3] Overall, 72% of enterprises now operate private clouds, often as part of a hybrid cloud strategy.[4]

Along with business agility and cost reduction, security and compliance rank high as reasons for private cloud deployment. Specifically, many organizations have elected to store sensitive or highly regulated data on their own resources to reduce the risk of data loss. Nevertheless, private clouds bring their own security issues, including:

1. **Full responsibility for security**, unlike the shared responsibility model with public cloud providers.
2. **Shifting workloads** between private clouds and public ones increase the risk of configuration errors and other security issues.
3. **Security breaches** are more common with private clouds than public ones, contrary to popular perception.[5]
4. **A lack of east-west visibility**, that is, into traffic within the network.

This eBook covers five key use cases for private cloud security and discusses how the Fortinet private cloud security solution provides effective solution for each use case.

Enterprises run 46% of their workloads in private clouds today.[6]

“The advantages of private cloud services are plentiful. But so are its hurdles. Understanding its promises and problems ... is crucial to use cloud effectively.”[7]

Intent-Based Segmentation: North-South L7 Advanced Security Protection

Protecting north-south traffic—that is, network traffic moving into and out of an enteprise or a data center—has long been recognized as a key element of enterprise security. The nature of today's advanced threats makes it doubly important. But the complexity of networking and the highly virtualized nature of private clouds brings new challenges in accomplishing it.

In addition, security teams are now impacted by business requirements for cost-effective, accelerated service delivery. Security protection for new services must be provisioned on the fly to meet time-to-market and performance targets. Otherwise, security-related delays can offset the efficiency and cost benefits realized by deploying a private cloud.

FortiGate-VM is a virtualized NGFW that provides advanced protection for north-south traffic in a virtualized environment such as a private cloud or a software-defined data center (SDDC). It automatically provisions and scales security in real time using zero-touch provisioning—no matter what is added to the infrastructure. It provides single-pane-of-glass management and visibility, eliminating operational silos while offering broad support for leading hypervisors, software-defined networking (SDN) solutions, and cloud platforms.

FortiGate-VM is integrated seamlessly into the Fortinet Security Fabric, which enables centralized visibility and control and full automation of security processes across a broad set of security solutions—powered by robust threat intelligence from FortiGuard Labs.

Of all types of security events, external attacks have by far the most damaging impact on organizations.[8]

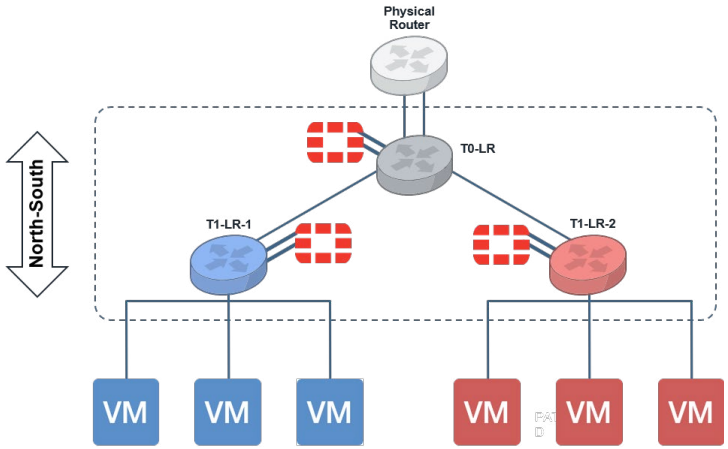

Figure 1: FortiGate-VM provides advanced protection for north-south traffic in the public cloud and an SDDC.

Intent-Based Segmentation: East-West L7 Advanced Security Protection

Many of the most damaging data breaches are accomplished by the lateral (east-west) movement of threat actors within a network.[9] As 68% of malicious intrusions are not discovered for months or longer,[10] cyber criminals often have a lot of time to find their way around a network, identifying the location of sensitive data and how to access it.

Network segmentation has long been used to control east-west traffic, but new complexities have arisen. Much network traffic now runs on the public internet using SDN, complicating entry points. Entities are no longer identified by a static IP address, making trust harder to determine. And private clouds are highly virtualized, meaning that segmentation cannot be done by physical servers. These complications require a more advanced approach to segmentation.

Microsegmentation is a method of creating secure zones in data centers and cloud deployments to isolate workloads from one another and secure them individually, restricting lateral movement within the network. FortiGate-VM NGFWs enable organizations to apply microsegmentation and control at the application layer. They enable deep packet inspection—both of encrypted and nonencrypted traffic—of east-west application and user traffic moving between virtual machines. Organizations can deploy granular policy segmentation across clustered resources, and policies can be set to sync across all FortiGate-VM NGFWs in real time using Fabric Connectors.

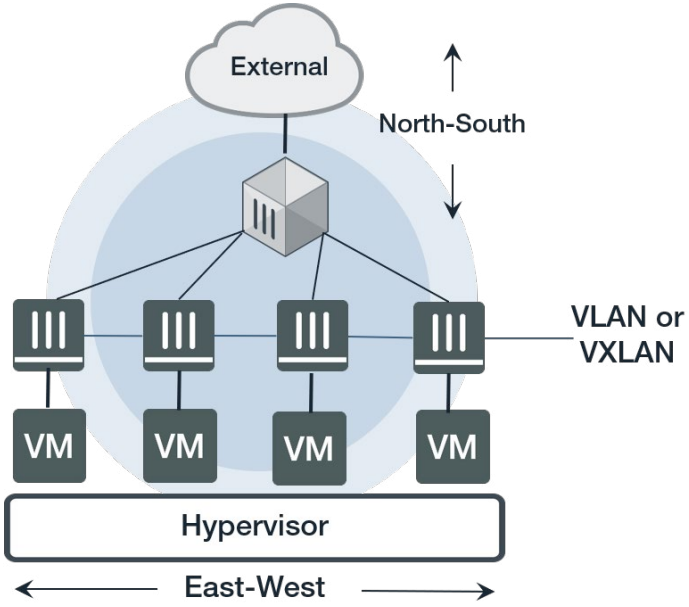

Figure 2: Microsegmentation protects against east-west movement of threats in the network using FortiGate-VM NGFWs.

“Researchers found that private clouds have 68% more security incidents than public clouds.”[11]

Form Factor Consolidation: Virtual Machine Preference

Companies electing to build private clouds have made a significant up-front investment with the expectation that it will yield dividends in long-term cost savings and the operational efficiencies of resource sharing. Inherent in the decision is a preference for VMs over physical machines for maximum flexibility and scalability on the fly.

The advantages of virtualization for these companies extend to the cybersecurity infrastructure. An organization that protects a private cloud infrastructure with hardware firewalls and security appliances is offsetting some of the efficiency and business agility gains realized through virtualization. It can also result in siloed operations between the security and network operations teams.

Fortinet offers virtualized versions of its FortiGate NGFWs and other network security elements. Importantly, the VM version of each solution delivers the same capabilities as a physical appliance, is based on the same FortiOS operating system, and is powered by the same advanced threat intelligence from FortiGuard Labs. Notably, the FortiGate-VM NGFW features the smallest footprint available in the marketplace,[12] boots within seconds, and delivers storage efficiencies for the maximum performance. This robust, virtual security infrastructure enables agile delivery of security protection for private cloud environments.

Figure 3: FortiGate-VM NGFWs provide companies with a cost-effective, highly flexible option for protecting their private clouds.

“Cloud computing actually makes things much more complex, not simpler. That requires a new discipline around managing that complexity.”[13]

Security Virtual Network Functions (VNF): Enabling Rapid Deployment

Companies that provide technology services have turned to virtual network functions (VNF) to enable rapid deployment of new network services to drive new revenue. Others are leveraging VNF technology to speed time to market for various initiatives. VNF handles specific network functions that run on one or more VMs on top of the hardware networking infrastructure. Individual VNFs can be connected or combined together as building blocks to offer a full-scale networking communication service.

Virtualization of customer premises equipment (CPE) enables Fortinet security solutions to be set up as a security VNF. FortiGate-VM can be deployed as a universal CPE (uCPE) at the on-premises edge or a virtual CPE (vCPE) hosted in the private cloud. VNF service chaining and orchestration is accomplished through partner orchestrators such as Amdocs, Nuage, and OpenStack. Specifically, service chaining is a capability that uses SDN capabilities to create a service chain of connected network services that are then connected in a virtual chain.

As a small-footprint security VNF with consolidated networking and security, FortiGate-VM offers a full Layer 7 security stack with intrusion prevention system (IPS), antivirus, web filtering, and secure SD-WAN features. Other elements of the Fortinet Security Fabric can be added, including email security, web application firewall, sandbox analysis, and more.

The global NFV market—hardware, software and services—will be worth $15.5 billion by 2020.[14]

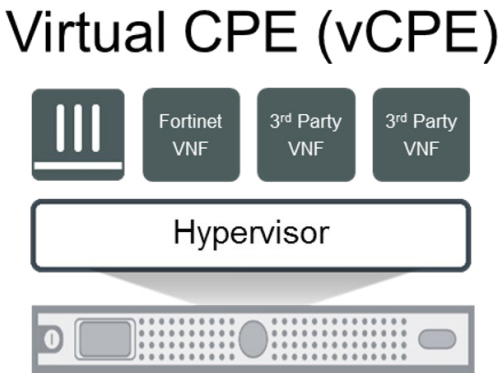

Figure 4: FortiGate-VM NGFWs deliver the same capabilities as physical appliances via a uCPE at the on-premises edge or vCPE hosted in the data center or public cloud.

Compliance and Governance: A Holistic, Centralized Approach

As more regulations are passed and media scrutiny of organizations' cybersecurity shortcomings intensifies, compliance is an increasingly important concern for almost every organization. For companies in highly regulated industries and those that handle a lot of personal data, compliance is a key reason for building a private cloud infrastructure in the first place. Some nations require that data generated in their country be kept in that country—something that is often difficult with public cloud providers. Others seek to avoid the steep fines and penalties imposed for noncompliance with newer regulations—especially the European Union's General Data Protection Regulation (GDPR) and similar laws in progress in other jurisdictions[15]—by keeping sensitive information out of public clouds for risk management reasons.

Without a comprehensive, integrated security architecture, compliance tracking and reporting can be a time-consuming, manual process. But Fortinet Security Fabric elements, such as FortiSIEM, FortiAnalyzer, and FortiManager, provide instant compliance reports, closed-loop compliance mitigation, and centralized management that enables organizations to implement changes across the infrastructure.

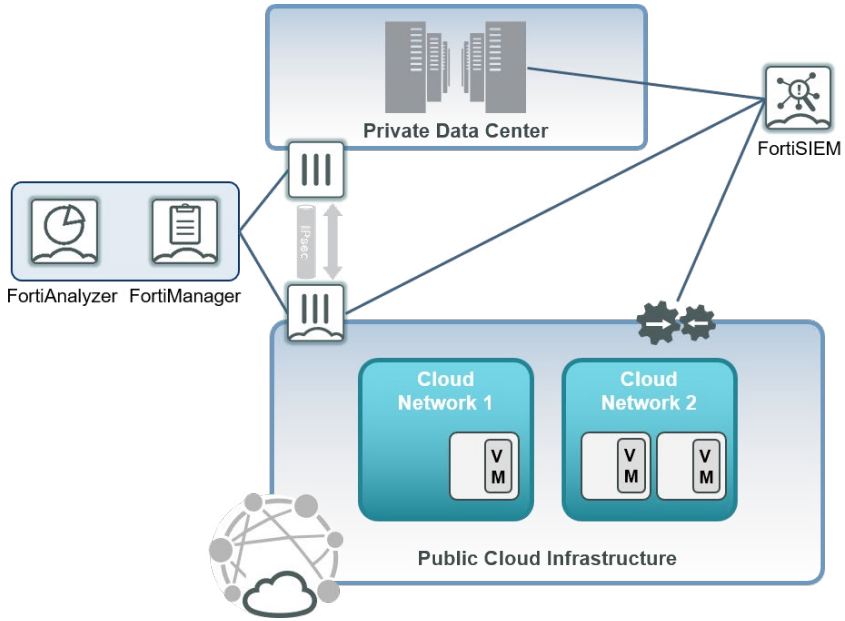

Figure 5: FortiSIEM, FortiAnalyzer, and FortiManager provide automated compliance auditing and reporting across cloud environments, which is combined with on-premises compliance data in a single-pane-of-glass view.

66%

of IT professionals say security and compliance are their greatest concerns in adopting an enterprise cloud computing strategy.[16]

Conclusion: Integrated Security in a Consistent Form Factor

An increasing number of organizations have elected to deploy private clouds to support operational efficiency, speed time to market, reduce cost, and ensure compliance. But this decision brings unique security challenges. As with other parts of a company's infrastructure, private clouds are best protected with a comprehensive, integrated security architecture with single-pane-of-glass visibility and control. And given the fact that private clouds are built on a virtual infrastructure, it is important that security solutions should be available in the virtual form factor—with all the features of the physical version.

For the private cloud and other virtualized environments, FortiGate-VM virtual NGFWs have the smallest footprint in the marketplace, ensuring that they actually contribute to the business agility envisioned for a private cloud deployment. FortiGate-VM integrates with Fortinet Security Fabric solutions that are also available in the virtual form factor. They enable effective protection for both north-south and east-west network traffic, and they can be configured as security VNFs. And associated Security Fabric tools help make compliance a proactive rather than a reactive endeavor. With Fortinet, organizations can build resilient public clouds without increasing risk.

"[P]rivate cloud deployments have many security advantages. However, 'advantages' does not mean organizations can forego due diligence."[17]

[1] "2019 RightScale State of the Cloud Report from Flexera: As Cloud Use Grows, Organizations Focus on Cloud Costs and Governance," RightScale from Flexera, accessed March 18, 2019.

[2] Marc Wilczek, "IT governance critical as cloud adoption soars to 96% in 2018," CIO, April 2, 2018.

[3] Ibid.

[4] "2019 RightScale State of the Cloud Report from Flexera: As Cloud Use Grows, Organizations Focus on Cloud Costs and Governance," RightScale from Flexera, accessed March 18, 2019.

[5] "Why Public Clouds are More Secure than Private Clouds," Dovel Technologies, accessed March 20, 2019.

[6] "2019 RightScale State of the Cloud Report from Flexera: As Cloud Use Grows, Organizations Focus on Cloud Costs and Governance," RightScale from Flexera, accessed March 18, 2019.

[7] Clive Longbottom, "Cutting through the promises and problems of private cloud services," Computer Weekly, accessed March 19, 2019.

[8] Kelly Bissell, et al., "Gaining Ground on the Cyber Attacker: 2018 State of Cyber Resilience," Accenture, April 10, 2018.

[9] For example, see Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," CSO, November 6, 2018.

[10] "2018 Data Breach Investigations Report," Verizon, accessed January 8, 2019.

[11] Eduard Kovacs, "Public Cloud Is Most Secure: Report," SecurityWeek, August 15, 2017.

[12] Based on internal research conducted by Fortinet.

[13] David Linthicum, "Cloud complexity management is the next big thing," InfoWorld, September 14, 2018.

[14] "Network Functions Virtualization Market Worth Over $15 Billion by 2020, Says IHS Markit," IHS Markit, July 19, 2016.

[15] Kassidy Kelley, "CCPA compliance begins with data inventory assessment," TechTarget, December 2018.

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

[17] Ed Moyle, "Private cloud computing security issues," TechTarget, accessed March 18, 2019.

www.fortinet.com

377550-0-0-EN

April 2, 2019 9:36 PM

eb-private-cloud-solution-selection