FORTINET

WHITE PAPER

Protecting the Cloud

Fortinet Technologies and Services that Address Your Cloud Security Challenges

Introduction

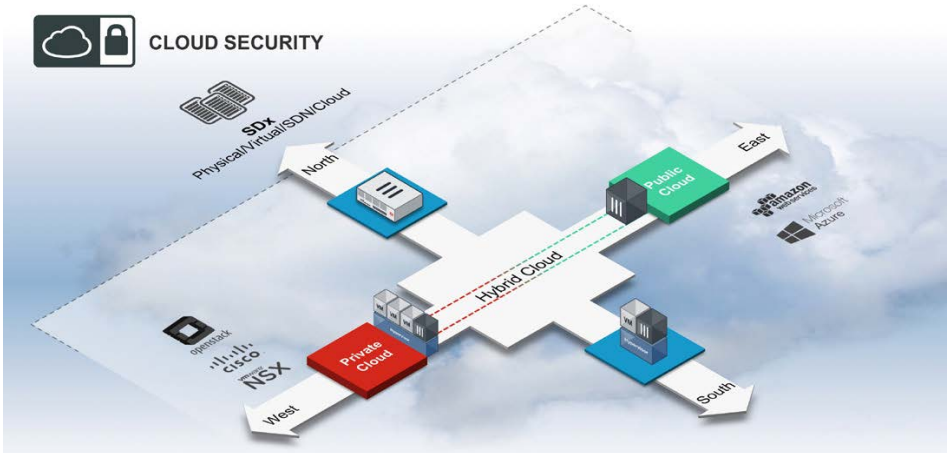
Given the constant pressure that CIOs are under to improve the return on investment (ROI) and reduce the total cost of ownership (TCO) of IT solutions, it should come as no surprise that the cloud has become one of the most talked-about topics in the industry. For example, the majority of 2015 predictions made by Gartner[1] involve the cloud and digital business in some way. Some notable Gartner predictions include:

These predications illustrate both the importance that companies are placing on cloud-based services as well as the challenges they face in securing those services.

Organizations need to ensure that data center designs cater to the use of mixed physical/software (cloud) appliance form factors and a blurring of traditional distinctions between cloud IaaS, infrastructure software, and data center hardware.

Organizations of all sizes are both excited by the opportunities the cloud provides and concerned about the challenges posed by moving data and applications to the cloud. In spite of the potential for increased ROI and lower TCO, securing data in the hybrid IT and cloud services is often cited as the number one concern by IT professionals looking to take advantage of cloud-based services[2].

This paper will explore the security considerations associated with moving to the cloud and discuss the key challenges associated with public and private clouds. It will also describe the technologies necessary to ameliorate current concerns regarding security in the cloud. Lastly, this paper will discuss Fortinet's ability to secure data moving to, from, and inside an organization's cloud infrastructure using the Fortinet Security Fabric to enable consistent security enforcement across the distributed network environment.



By 2018, 20% of new technology spending will be on fully integrated, platform-based solutions, offered with as-a-service pricing models.

By 2018, 15% of the business services market spending will be derived through hybrid IT and cloud services brokerage models.

By 2018, data center managers will not care which vendor's server is running 20% of their private data center workloads, up from virtually zero today.

Which Cloud to Choose?

The first issue to consider as you look towards the cloud is which architectural approach you want to take in adopting cloud services. The classes of cloud architecture are public, private, hybrid, and community.

Public Clouds

Public clouds are available to any organization, and a variety of well-known vendors including Microsoft, Rackspace, Symantec, and Amazon provide these public cloud environments. They are designed to provide the following benefits:

Scalability – Users have the ability to access additional compute resources on demand in response to increased application loads.

Flexibility – Public cloud provides flexible, automated management to distribute the computing resources among the cloud's users.

Reliability and fault tolerance – Cloud environments can take advantage of their large numbers of servers by enabling applications to utilize built-in redundancy for high availability.

Utility-based computing – Users only pay for the services they use, either by subscription- or transaction-based models.

Shared resources – By enabling the consolidation of IT resources, multiple users share a common infrastructure, allowing costs to be more effectively managed.

CAPEX savings – Because the vendor is providing all the hardware, software, support, security, and high availability for the infrastructure, the organization pays only to use the service, saving significant capital expenditures.

In spite of the many advantages of a public cloud, you still need to exercise caution before moving to a public cloud.

The primary concerns with public clouds are:

Data access and control – Whenever data moves outside the walls of the organization, concerns over the privacy and security of the data will come up. While many cloud providers have extensive security measures deployed in their data centers, it is important to research potential cloud providers and fully vet their data security practices to ensure they are best of breed. The Cloud Security Alliance (CSA) provides guidance for both governance and operational areas that should be evaluated before moving to the cloud[3].

Vendor lock-in – Once you move your data and applications to the cloud, it can become very difficult to move away from that provider. To reduce this risk, administrators should investigate the process for extracting data from the cloud service provider and structure their data in a way to expedite a future transition to another provider if necessary.

Vendor lock-in – Once you move your data and applications to the cloud, it can become very difficult to move awayfrom that provider. To reduce this risk, administrators should investigate the process for extracting data from the cloud service provider and structure their datain a way to expedite a future transition to another provider if necessary.

Reliability – In theory, public clouds offer higher availability than traditional premisesbased networks because the vendor is providing SLAs around this availability and has a financial interest in delivering it. Unfortunately, even public clouds can fail if not designed properly, leaving customers without access to their own data and applications. Customers must be very familiar with the service-level agreements of their providers and should have plans in place to address any outage.

Ultimately, cloud-based services can help you better manage your organization's computing resources by providing flexibility and scalability. There are numerous examples of organizations using public clouds to quickly stand up applications requiring a significant amount of computing resources, all without having to plan and invest in their own internal infrastructures.

Private Clouds

As the name suggests, private clouds are designed to be visible only to the organization that creates them. Private clouds provide many of the same benefits that a public cloud does, and still allows you to maintain ownership of the data and equipment. A private cloud is essentially a private data center that an organization creates with stacks of servers all running virtual environments, providing a consolidated, efficient platform on which to run applications and store data.

Private clouds allow you to reap many of the benefits of cloud computing – scalability, metering, flexible resource allocation, and so forth – without exposing any of your organization's assets to the public Internet. Private clouds also address some of the top concerns that prevent some organizations from moving to the cloud. Since the data stays internal to the organization, concerns about vendor lock-in and regulatory compliance are minimized.

However, where private clouds differ from public clouds is that private clouds usually require a significant investment to plan and deploy. The following are all costs that you should consider as you look to create a private cloud:

Hardware and software – To create a private cloud, an organization must purchase all the servers, virtualization software, application licenses, and networking hardware to create the private cloud. The organization must also bear the costs of upgrading resources as the cloud grows.

Additional help desk resources – As users move data and applications to the cloud, the number of help desk requests will rise. It will require extra support and training during the migration process.

Specialized IT skills – Unfortunately, a private cloud does not administer itself, and the skill set required for the IT department to deploy, manage, and maintain a cloud environment will be different from the skill set it utilizes for its on-premises systems. Potential solutions to the need for specialized skills could include hiring a consulting firm, training existing staff, and hiring new employees (or a combination of all three options) to manage the new infrastructure.

High availability and disaster recovery – You will have to invest in additional resources to ensure that the private cloud maintains full-time availability and is fault tolerant. This will require extra investment on redundant systems, and may include construction of duplicate facilities when the primary facility is located in a highrisk area.

Reduced economies of scale – Although a large organization will reap the benefits of scalability and flexible resources using a private cloud, the efficiencies and cost savings will be limited by the company's size.

Despite these challenges, private clouds can provide significant advantages to organizations that need the flexibility and on-demand resources offered by the cloud, but cannot move the data outside of the organization.

Hybrid and Community Clouds

Hybrid and community clouds are cloud architectures that incorporate components of private and public clouds, depending on their use cases. NIST defines these two architectures as[4]:

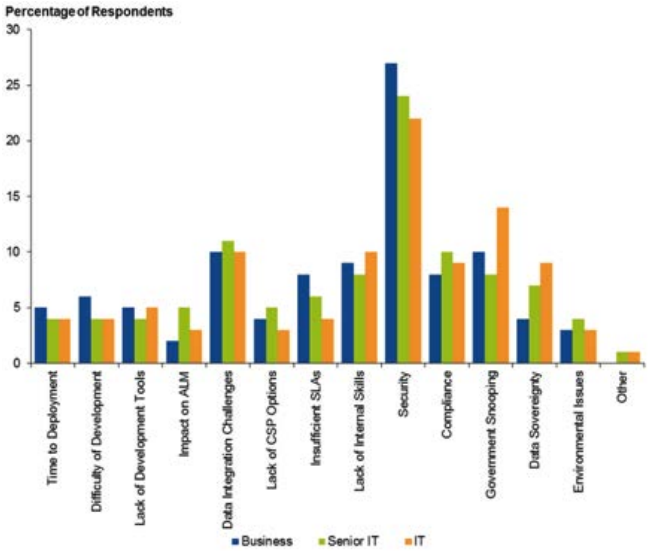
Hybrid Clouds – The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Community Clouds – The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Cloud Security Concerns

There are a variety of security challenges related to both private and public cloud computing. Data loss, data breaches (loss of personal or credit card information), unsecure application programming interfaces (APIs) between cloud-based and traditional businesses, and shared technology in a multi-tenant environment are just a few of the concerns expressed by a respondent tackling the option of using public cloud.

Figure 1 below shows the top-ranked challenges related to cloud security as indicated by Gartner in 2014.



n = 210
ALM = application life cyclelifecycle management
CSP = communication services provider
SLA = service-level agreement
Source: Gartner (October 2014)

Figure 1: Security and Privacy Concerns Lead the Reasoning for Hybrid Computing Models, 2014

With the exposure of sensitive data and data loss listed as the two most common concerns related to cloud security, it is imperative that you look carefully at how your organization's data will be protected as it enters, travels through, and leaves the `cloud.

Securing Data Entering and Leaving the Cloud

Data entering and leaving the cloud should be subject to the same level of scrutiny as any other data entering or leaving the network. Critical network security technologies such as firewall, intrusion prevention, application control, and content filtering need to provide that level of scrutiny. A security fabric approach allows organizations to share threat intelligence and coordinate countermeasures between local and cloud-based security solutions.

The additional challenge associated with securing data in the cloud is that the security architecture must also secure the multi-tenant nature of the traffic. This means the security architecture must have the ability to enforce separate policies on traffic, depending on origin or destination. The security technologies in place must also have the ability to keep traffic entirely separate in order to avoid any risk of unauthorized access.

Securing Data in the Cloud

Once data is in the cloud, new challenges around security emerge. Primary among this is the need to maintain control over data as it flows from virtual machine to virtual machine. Unlike with an integrated Security Fabric approach, traditional security hardware-based appliances have no control over the data once in the cloud, which requires the presence of virtual security appliances to inspect and protect the data in the virtualized environment.

The additional challenge associated with securing data in the cloud is that the security architecture must also secure the multi-tenant nature of the traffic. This means the security architecture must have the ability to enforce separate policies on traffic, depending on origin or destination. The security technologies in place must also have the ability to keep traffic entirely separate in order to avoid any risk of unauthorized access.

Vulnerabilities of the Cloud

Cloud environments are by design fluid, and therefore require regular updates to the security architecture to ensure protection. Despite efforts by cloud providers to stay abreast of the latest threats, a single zeroday vulnerability could provide the means with which to potentially compromise every customer and machine being hosted within the cloud provider's network.

In order to address this risk, cloud providers need to invest in security vendors that provide frequent updates and a global intelligence network that can accurately identify and protect against new vulnerabilities and attacks before they are exploited in the wild. When security provided by a cloud provider matches network solutions, organizations can share threat intelligence, establish consistent policies, and coordinate responses, across the entire Security Fabric.

Fortinet's Multi-tenant Architecture

Virtual domains (VDOMs) are a method of dividing a Fortinet® FortiGate® physical or virtual appliance into two or more virtual units that function independently. VDOMs can provide separate network security policies and completely separate configurations for routing and VPN services for each connected network or organization. This native ability to split a single FortiGate device into multiple secure entities provides the enhanced levels of security and data segmentation needed to build any cloud architecture. Some key advantages of FortiGate VDOMs are:

Easier Administration

VDOMs provide separate security domains that allow separate zones, user authentication, firewall policies, routing, and VPN configurations. VDOMs separate security domains and simplify administration of complex configurations as security administrators do not have to manage as many settings at one time. This is critical for complex networks that might have different administrators for different functional domains or for different groups of devices.

Enabling Customers to Build and Maintain Secure Clouds

Fortinet, the leader of the worldwide unified threat management market[5], has a variety of products designed to extend traditional network security protection into the cloud as standalone solutions, or as part of Fortinet's distributed Security Fabric architecture. As described previously, the only way to mitigate fears of moving to the cloud is to ensure that protection is in place at all points along the path of data: entering or exiting the corporate network, entering or exiting the cloud, and within the cloud.

VDOMs also provide an additional level of security because regular administrator accounts are specific to one VDOM — an administrator restricted to one VDOM cannot change information on other VDOMs. Any configuration changes and potential errors will apply only to that VDOM and limit any potential down time. Using this concept, you can further split settings so that the management domain is only accessible by a single admin and does not share any settings with the other VDOMs.

Continuous Security

VDOMs also provide a continuous path of security. When a packet enters a VDOM, it is confined to that specific VDOM and is subject to any firewall policies for connections between that VDOM and any other interface. When hosting separate clients or entities on a single cloud architecture (very common with public and community clouds), the ability to guarantee that no data can pass from one connection to another is a critical requirement.

These provide the unique differentiation to help enterprise and cloud service providers to construct private and hybrid cloud with most effective resources and budget.

Savings in Physical Space and Power

Data entering and leaving the cloud should be subject to the same level of scrutiny as any other data entering or leaving the network. Critical network security technologies such as firewall, intrusion prevention, application control, and content filtering need to provide that level of scrutiny. A security fabric approach allows organizations to share threat intelligence and coordinate countermeasures between local and cloud-based security solutions.

The additional challenge associated with securing data in the cloud is that the security architecture must also secure the multi-tenant nature of the traffic. This means the security architecture must have the ability to enforce separate policies on traffic, depending on origin or destination. The security technologies in place must also have the ability to keep traffic entirely separate in order to avoid any risk of unauthorized access.

Securing Data in the Cloud

Once data is in the cloud, new challenges around security emerge. Primary among this is the need to maintain control over data as it flows from virtual machine to virtual machine. Unlike with an integrated Security Fabric approach, traditional security hardware-based appliances have no control over the data once in the cloud, which requires the presence of virtual security appliances to inspect and protect the data in the virtualized environment.

The additional challenge associated with securing data in the cloud is that the security architecture must also secure the multi-tenant nature of the traffic. This means the security architecture must have the ability to enforce separate policies on traffic, depending on origin or destination. The security technologies in place must also have the ability to keep traffic entirely separate in order to avoid any risk of unauthorized access.

Vulnerabilities of the Cloud

Cloud environments are by design fluid, and therefore require regular updates to the security architecture to ensure protection. Despite efforts by cloud providers to stay abreast of the latest threats, a single zeroday vulnerability could provide the means with which to potentially compromise every customer and machine being hosted within the cloud provider's network.

In order to address this risk, cloud providers need to invest in security vendors that provide frequent updates and a global intelligence network that can accurately identify and protect against new vulnerabilities and attacks before they are exploited in the wild. When security provided by a cloud provider matches network solutions, organizations can share threat intelligence, establish consistent policies, and coordinate responses, across the entire Security Fabric.

Savings in Physical Space and Power

FortiGate VDOM technology allows you to increase the number of domains protected without having to increase the amount of rack space and power consumed. There is no need to make physical changes to the network to accommodate additional customers or domains. Also, there is no risk of expensive hardware sitting around idle if growth projections prove to be inaccurate.

Increasing VDOMs involves no additional hardware, no additional cabling, and very few changes to existing networking configurations. Your ability to create virtual domains is limited only by the size of the VDOM license you purchase and the physical resources of your FortiGate device.

Virtualized Products

Fortinet has a wide range of virtualized products for many of its hardware platforms as well as traditional physical appliances that can be deployed individually, or interconnected with other physical or virtualized solutions to support a Security Fabric architectural strategy. Fortinet virtual appliances allow you to scale quickly to meet demand and protect intra-virtual machine communications by implementing critical security controls within your virtual infrastructure, running on leading hypervisors like VMware ESXi and Citrix Xen as well as OpenStack for agile deployment instantly. Fortinet provides virtualized appliances for the following product families:

Cloud Compatible

FortiGate-VM is certified with Amazon AWS, Microsoft Azure, HPE Helion Cloud platforms. In the hybrid IT environment, Fortinet enables hourly metering, annual pay-as-you-go subscription, and bring-your-own-license (BYOL) perpetual license to embrace the complete security portfolio in varying cloud deployments.

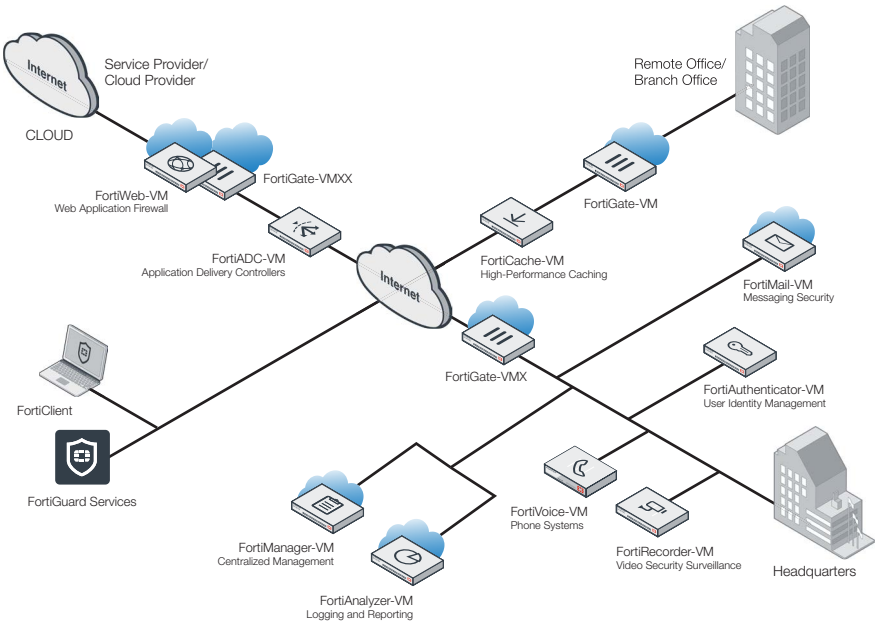
FortiGate – Fortinet's flagship network security solution that delivers the broadest range of consolidated network security and network services on the market, including:

- Firewall, VPN, and Traffic Shaping
- Intrusion Prevention System (IPS)
- Antivirus/Anti-spyware/Anti-malware
- Integrated Wireless Controller
- Application Control
- Data Loss Prevention (DLP)
- Vulnerability Management
- Dual-Stack IPv6 Support
- Web Filtering
- Anti-spam VoIP Support
- Dual-Stack IPv6 Support

FortiManager™ – "Single-pane-of-glass" management console for configuring and managing any number of Fortinet devices, from several to thousands, including FortiGate®, FortiWiFi™, FortiCarrier™, FortiMail™, and FortiAnalyzer™ appliances and virtual appliances, as well as FortiClient™ endpoint security agents. You can further simplify control and management of large deployments by grouping devices and agents into administrative domains (ADOMs).

FortiAnalyzer – Centralized logging, analyzing, and reporting appliances securely aggregate log data from Fortinet devices and other syslog-compatible devices. A comprehensive suite of easily customized reports enables you to analyze, report, and archive security event, network traffic, web content, and messaging data to measure policy compliance.

FortiWeb™ – FortiWeb web application firewalls protect, balance, and accelerate your web applications, databases, and any information exchanged between them. Whether you are protecting applications delivered over a large enterprise, service provider, or cloud-based provider network, FortiWeb appliances will reduce deployment time and simplify security management.



FortiMail – FortiMail prevents your email systems from becoming threat delivery systems. Its inbound filtering engine blocks spam and malware before it can clog your network and affect users. Its outbound inspection technology prevents other anti-spam gateways from blacklisting your users by blocking outbound spam and malware, including mobile traffic.

Unmatched Protection

Each FortiGate virtual appliance ships with the broadest range of security and network technologies of any virtual appliance on the market today. And, because all of these technologies are included with the FortiGate-VM license, you have complete flexibility to deploy the right mix of technologies to fit your unique virtualized environment and address concerns about migrating data to the cloud.

Each FortiGate-VM delivers the same comprehensive suite of consolidated, integrated security technologies as the industry-leading FortiGate physical appliances. This suite includes:

- The latest enterprise firewall technologies like IPv4/IPv6 firewall, application control, and intrusion prevention, which deliver unmatched granular management and control of data, applications, users, and devices.
- Technologies to block today's spear phishing attacks, APTs, and other targeted attacks, such as anti-spam, antivirus, web content filtering, and data loss prevention.
- Essential protection for remote users and offices such as VPN, endpoint protection, two-factor authentication, and vulnerability management.
- Core networking support, such as IPv4/ IPv6 dynamic routing, WAN optimization, traffic shaping, and VoIP.

Fortinet Platform-based Solution

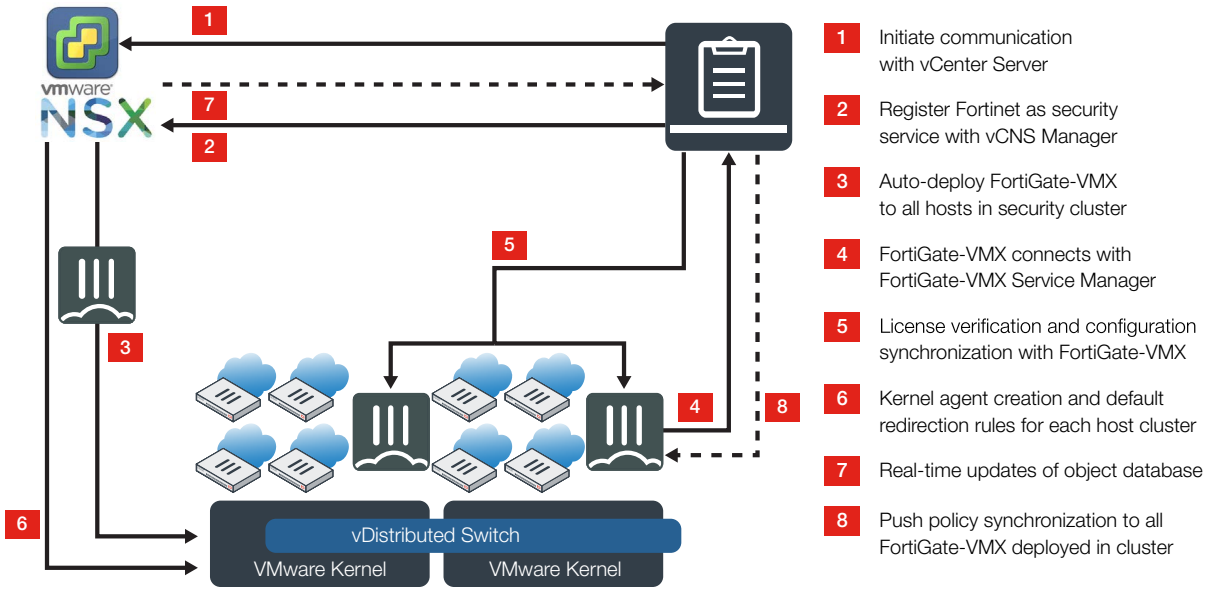
The FortiGate-VMX solution is purpose-built for the VMware NSX network virtualization platform to separate FortiGate-VMX Service Manager control plane via API provided by VMware and to enable the VMware's NSX Manager to deploy FortiGate-VMX appliances as soon as rules are applicable and hosts are added. The technology supports virtual machine migration (vMotion) to ensure no rules are dropped when workloads are changed. The solution avoids traditional manual security rule hairpinning and helps scale and provision automatically with the data center's growth as needed.

Further, with advanced API integration, FortiGate Connector for Cisco ACI (Application Centric Infrastructure) is the Fortinet solution to provide seamless integration between Fortinet Firewall (FortiGate) deployment with Cisco APIC (Application Policy Infrastructure Controller). This integration allows customers to perform single point of FortiGate configuration and management operation through Cisco APIC.

The same implementation can also be extended to any other hypervisors where software-defined extensibility is available.

FortiGuard Services

The FortiGuard® Labs global team of threat researchers continuously monitors the evolving threat landscape.



The 200+ dedicated researchers provide around-the-clock coverage and updates to ensure the most to-date protection possible. The FortiGuard Labs team delivers rapid product updates and detailed security knowledge, providing protection from new and emerging threats. Our research team has locations in the Americas, Europe, and Asia.

The FortiGuard Labs team provides updates to a variety of Fortinet services, including:

- Intrusion Prevention
- Antivirus
- Database Security
- Web Filtering
- Application Control
- Anti-spam
- Web Security

Fortinet Analysis and Management Services

These services, in conjunction with Fortinet research analysts, provide a constant stream of up-to-date signatures and prevention measures against potential attacks. When protecting a cloud-based environment, it is imperative to have timely protection in place against any attack that might occur within a physical or virtual environment.

Fortinet Secures the Breadth of Deployment Options in the Cloud

Cloud computing is all about elasticity scalability and orchestration automation. Choosing the appropriate cloud architecture is only the first step in the transition to virtualized deployments. The next step is for you to determine which services will be deployed in the cloud and how physical and virtual components will interact. One of the key strengths of virtualized technology is the ability to provide flexible, scalable computing for a variety of services, and your network security solution has to be equally flexible and scalable. As requirements for processing change, you need to be able to make changes on demand to both your cloud environment and the security solution protecting that environment.

Fortinet products provide agile end-to-end security regardless of the deployment option. As you look to a combination of physical and virtualized solutions to solve your contemporary IT challenges, it is essential to select a single security solution that can protect your evolving network with consistent and collaborative intelligence and enforcement regardless of where it is deployed.

With the broadest portfolio of physical and virtual appliances in the industry, all controlled by a single unified management platform, Fortinet allows you to secure a wide variety of cloud and network configurations, including the integrated Fortinet Security Fabric. Some popular network deployments that Fortinet can protect are:

Hosted Services

Hosted services include software as a service (SaaS), infrastructure as a service (IaaS), platform as a service (PaaS), and many others (referred to as XaaS or “anything as a service”6). Each of these services requires the same specialized security that exists in the physical realm as well as unique attributes to operate in a virtualized environment.

With these distinct Fortinet products available in a virtual appliance form factor, you can provide dedicated security regardless of the service offering. For example, virtual FortiMail and FortiWeb appliances can protect your web and email servers. FortiAnalyzer can provide the log-analytics and centralized PCI compliance reporting package. FortiGate can provide proven protection for your entire virtual infrastructure. And for even more tightly coordinated security, they can be woven into a Fortinet Security Fabric architecture.

Software-defined Networking

Protecting individual services is only one part of the equation. Another popular trend, driven by cloud computing and virtualization, is Software-Defined Networking (SDN). SDN is an approach to networking in which control is decoupled from hardware and given to a software application called a controller[7]. SDN enables rapid changes in switching and routing policies independent of physical architecture, meaning that security policies can easily become out of date, leading to gaps in protection.

Virtualized Fortinet appliances are well-suited to enabling and protecting SDN environments. Fortinet products support the routing protocols and VPN technology necessary for administrators to implement new infrastructures while maintaining proper security policies.

Virtualized FortiGate devices support dynamic routing protocols in both IPv4 and IPv6 (such as BGP and OSPF), allowing administrators to define new network routes as necessary. Built-in IPsec and SSL VPN technologies allow you to protect new connections to data centers and encrypt and secure communication between systems and end users.

Conclusion

The popularity of cloud-based services and the high risk associated with moving data into and across the cloud has companies of all sizes looking for solutions to address their cloud computing challenges. Securing the cloud requires a variety of technologies, and no single technology can address all the challenges. Cloud providers and customers must take special care to understand all the safeguards in place with any cloud solution, whether considering an individual solution or an integrated Security Fabric strategy.

Fortinet's Security Fabric expands that capability by integrating security for the cloud with customer access layer, network, application, data center, and content security into a single collaborative solution that can be orchestrated through a single management interface. This cloud security product strategy is purpose-built around a multi-tenant architecture. Fortinet has the breadth and depth of solutions to address securing applications and data as they move to, through, and outside of the cloud. By providing centrally managed physical and virtual appliances that deliver the broadest range of network security solutions in the industry, Fortinet can help protect your critical data from the customer to the cloud and back.

[1] http://www.gartner.com/technology/research/predicts/

[2] http://searchcloudsecurity.techtarget.com/news/2240031767/Cloud- compliance-cloud-encryption-top-enterprise-security-concerns

[3] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[4] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5] IDC

[6] http://searchcloudcomputing.techtarget.com/definition/XaaS-anything-as- a-service

[7] http://whatis.techtarget.com/definition/software-defined-networking-SDN

FORTINET

www.fortinet.com

October 30, 2019 2:05 AM

488925-A-0-EN

D:\Fortinet\White Paper\refresh - Protecting the Cloud\wp-protecting-the-cloud