FORTINET

SOLUTION GUIDE

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 2012 predications made by Gartner[1] involved the cloud in some way. Some notable Gartner predictions include:

> **"By 2015, low-cost cloud services will cannibalize up to 15 percent of top outsourcing players' revenue."**
>
> **"By 2016, 40 percent of enterprises will make proof of independent security testing a precondition for using any type of cloud service"**
>
> **"At year-end 2016, more than 50 percent of Global 1000 companies will have stored customer-sensitive data in the public cloud."**

These far-reaching 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 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 cloud 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.

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 private, public, community, and hybrid.

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 number of servers by enabling applications to utilize this built- in redundancy for high availability and redundancy.
>
> **Utility-based computing** - Users only pay for the services they use, either by subscription or transaction-based models.

---

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

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

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 around 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 datacenters, 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 around 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.

Regulatory compliance – Some compliance bodies have not updated their standards with provisions for cloud-based data. This does not necessarily prevent you from moving your organization's data and applications to the cloud, but you must investigate whether a cloud provider's infrastructure, processes, data access and storage policies meet your compliance requirements. Another option is to ask potential cloud providers if they have companies with similar compliance issues using their service, and investigate how those companies have satisfied compliance and audit requirements.

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

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

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 datacenter 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

---

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

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 around 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 much 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-premise 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 high-risk 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 case. 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.

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

Cloud Security Concerns

There are a variety of security challenges related to both private and public cloud computing. Figure 1 below shows the top-ranked challenges related to cloud security as indicated by Information Security professionals in a 2011 $(ISC)^2$ survey.

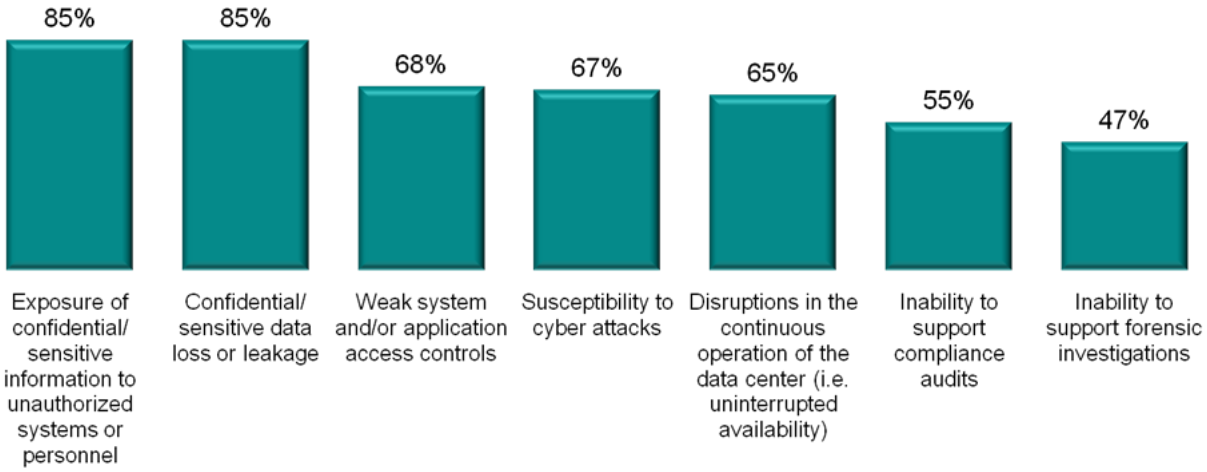


Figure 1 - Concerns around moving to the cloud

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 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.

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. Traditional 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.

Vulnerabilities and the Cloud

Cloud environments are by design fluid, and therefor require regular updates to the security architecture to ensure protection. Despite efforts by cloud providers to stay abreast of the latest threats, a single zero-day 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 identity and protect against new vulnerabilities and attacks before they are exploited in the wild.

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 described previously, the only way to mitigate fears around 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 itself.

Fortinet's Multi-Tenant Architecture

Virtual domains (VDOMs) are a method of dividing a 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 segregation 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.

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.

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.

---

[5] IDC (www.idc.com)

Virtualized Products

Fortinet has a wide range of virtualized products for many of its hardware platforms as well as traditional physical appliances. 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 both VMware and Citrix XenServer. Fortinet provides virtualized appliances for the following product families:

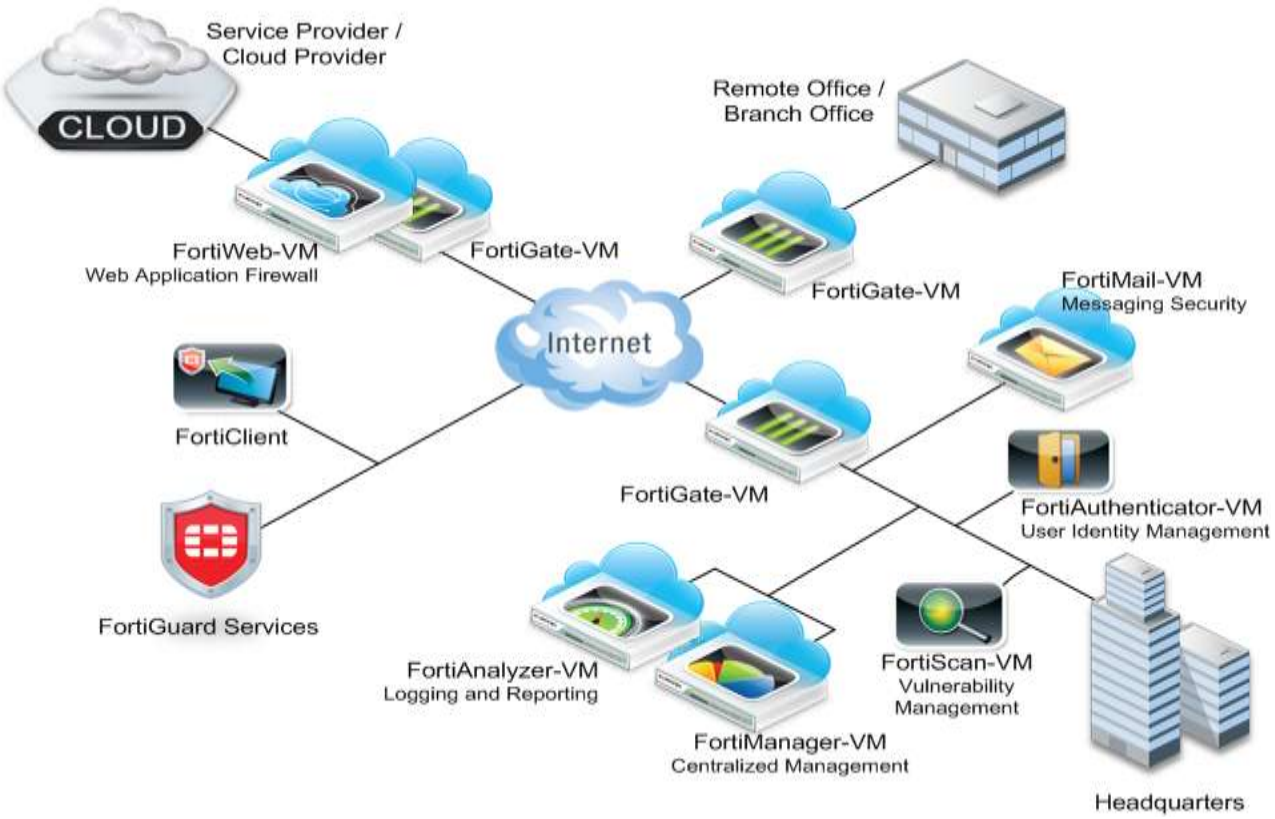
- FortiGate – Fortinet's flagship network security solution that delivers the broadest range of consolidated network security and network services on the market, including:
  - Firewall, VPN, and Traffic Shaping
  - Intrusion Prevention System (IPS)
  - Antivirus/Antispyware/Antimalware
  - Integrated Wireless Controller
  - Application Control
  - Data Loss Prevention (DLP)
  - Vulnerability Management
  - Dual-Stack IPv6 Support
  - Web Filtering
  - Antispam
  - VoIP Support
  - Layer 2/3 Routing
  - WAN Optimization & Web Caching
- 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 aggregates 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.
- FortiMail - Proven, powerful messaging security platform for any size organization, from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, the FortiMail solution utilizes Fortinet's years of experience in protecting networks against spam, malware, and other message-borne threats.
- 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.
- FortiScan™ - Enables your organization to close IT compliance gaps and implement continuous monitoring for real-time results. FortiScan provides you with an enterprise-scale solution that integrates endpoint vulnerability management, industry and federal compliance, patch management, remediation, auditing and reporting into a single, unified platform.

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 next-generation firewall (NGFW) 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 spearphishing attacks, APTs, and other targeted attacks such as Antispam, Antivirus, Web Content Filtering, and Data Leak 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

Figure 2 - The Fortinet Virtualized Product Portfolio

FortiGuard Services

The FortiGuard® Labs global team of threat researchers continuously monitors the evolving threat landscape. The 150+ dedicated researchers provide around-the-clock coverage and updates to ensure the most up 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
- Antispam
- Web Security
- Fortinet Analysis and Management Services
- Vulnerability Control and Management

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

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-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 both your evolving network.

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. 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 seven 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, FortiScan can protect your virtual platforms against vulnerabilities by FortiScan, and FortiGate can provide proven protection for your entire virtual infrastructure.

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. Software Defined Networking (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.

---

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

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

Conclusion

The popularity of cloud based services and the high risk associated with moving data to 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 around any cloud solution.

Fortinet 's network security product strategy is purpose-built around a multi-tenant architecture. Fortinet has the breadth and depth of solutions to address securing data as it moves to, through, and outside of the cloud. By providing centrally managed physical and virutal appliances that delvier 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.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1 408 235 7700
Fax +1 408 235 7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33 4 8987 0510
Fax +33 4 8987 0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784