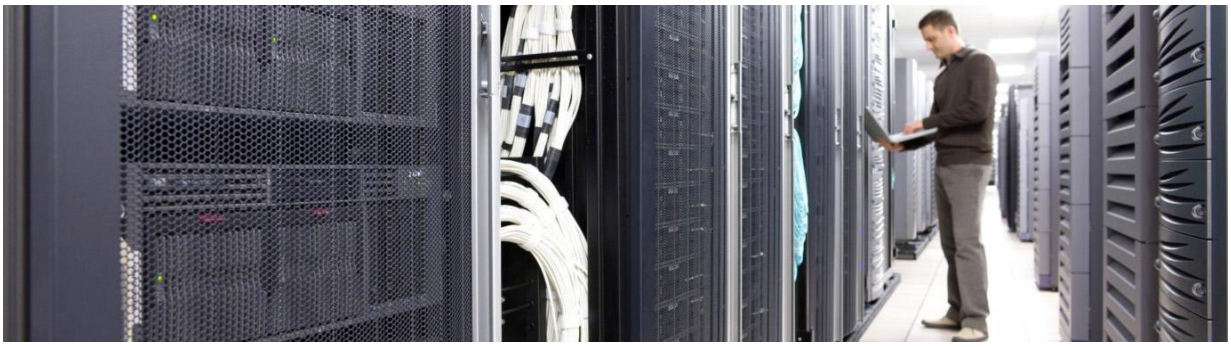
White Paper

Cisco Data Center Security Mitigates Risk When Transitioning to the Private Cloud



Cloud computing is gaining attention as the next step in IT evolution. While cloud computing has many benefits, such as increased business agility, scalability, efficiency, and profitability, it also introduces new security risks and concerns. These challenges are complex because they involve not only technology issues but also substantial process changes stemming from the new business computing models involved.

Rather than rejecting the cloud outright, many leading-edge companies are turning to private cloud models, taking a strategic and architectural approach in order to meet their business requirements while implementing policy enforcement and compliance controls that are consistent across data center boundaries. In this white paper, we will provide an overview of cloud models and explain the benefits of private clouds, the barriers to cloud computing, critical considerations for minimizing risk in private cloud deployments, and how Cisco can help you make this transition.

Cloud Characteristics and Models

According to the National Institute of Standards and Technology (NIST), there are five cloud characteristics and four cloud deployment models.

Cloud characteristics include:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed and automatically, without requiring human interaction with each service provider.
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction. Examples of resources that can be pooled include storage, processing, memory, and network bandwidth.

- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service:** Cloud-computing systems automatically control and optimize resource use through a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, tablets, laptops, and workstations).

Cloud deployment models include:

- **Community cloud:** A community cloud shares infrastructure between several organizations from a specific community with common concerns (for example, security, compliance, or jurisdiction). A community cloud can be managed internally or by a third party and can be hosted internally or externally.
- **Public cloud:** With a public cloud, the cloud infrastructure is provisioned by the cloud provider for open use by any type of customer. The infrastructure may be owned, managed, and operated by a business, academic, or government organization, or some combination of these entities.
- **Private cloud:** In a private cloud, the infrastructure is provisioned solely for a single organization and may be managed internally or by a third party and hosted externally (as a virtual private cloud). Also in a private cloud, multiple business units can be separated by multitenants. The provider has full knowledge of resource locations as they own the infrastructure.
- **Hybrid cloud:** A hybrid cloud is composed of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. A hybrid cloud can also consist of multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.

Business Benefits for Moving to the Private Cloud

Unlike traditional physical, on-premises data centers where applications are bound to a static server, private cloud models offer reduced cost and increased business agility, efficiency, and scalability. Among companies that can choose between public, hybrid, or private cloud models, many are turning to the private cloud because this model can address their concerns about security, compliance, and policy. According to the CSO Cloud Computing Survey 2012, 23 percent of respondents reported that their organization has information residing in a private cloud. This makes private clouds the most popular cloud-computing model, with the hybrid model, at 11 percent, coming in second.[1]

Private clouds offer many benefits to the enterprise. These benefits include self-service provisioning that matches or exceeds that of third-party providers; applications and services tailored to specific business needs; trusted security and compliance that is currently unavailable from public cloud providers; and the ability to scale resources with automatic provisioning to permit high utilization and high agility. Private clouds can also decrease costs by consolidating workloads to optimize server utilization while maintaining performance and agility.

[1] Bragdon, Bob, 2012 CSO Cloud Computing Study, June 19, 2012, page 6.

In calculating the cost advantages of private clouds, cost comparisons between public and private clouds show that for enterprises with significant resources in place, the move to private clouds can be up to 40 percent less expensive than moving to the public cloud.[2]

Barriers to Moving to the Cloud

Security is currently the top barrier to moving to the cloud. According to the CSO survey, 68 percent of enterprises are not confident that data placed in the cloud is secure. The following are some common security concerns about moving to the cloud.

Information Security

- **Multitenancy:** Whereas small, distributed data centers host a small number of applications or support a single organization, today's consolidated data centers and clouds have disparate user groups that require complete separation of network traffic and strict access control policies, even though they are sharing the same physical servers and network infrastructure. This is also true of private virtual data centers and private clouds, where internal tenants require virtual or physical separation.
- **Data at rest and data in motion:** Mobility of applications between servers, remote data centers, and clouds introduces complexity in the network security layer, which has typically relied on fixed-resource locations and static private networks to enforce security policies. Flexibly moving security policies along with virtual workloads has been challenging.

Access to Data and Applications

- **Identity and authorization:** In a world of increasing mobility, unsecured devices, and increasingly sophisticated threats, the network must take over many security policy enforcement responsibilities from applications. Therefore, the network infrastructure is performing more user authentication and access policy authorization enforcement, assuming these functions from application endpoints as networks become more context-aware and application-aware. The network security infrastructure is increasingly required to enforce identity-based and role-based policies, and to make other contextual decisions. The capability to block traffic to an application or server in the data center or cloud can no longer be based on the typical source or destination addresses of hosts. Now it must be based on the identity or role of the user, the process, or the application in the transaction.
- **Local and remote access:** Access can also depend on context-specific attributes in addition to identity, including the type of device accessing the application, the location of the user, the time of the request, and more. These context-aware policies are increasingly becoming the responsibility of the data center firewall and intrusion prevention system (IPS), which have to expand their capabilities to detect devices and control access based on these policies, as well as to monitor for the presence of malware, unauthorized access attempts, and sophisticated attacks. The modern enterprise runs a wide array of mission-critical commercial and highly customized applications. The data within those applications is a high-value target for attackers, yet access to that data is what drives the productivity and success of the enterprise.

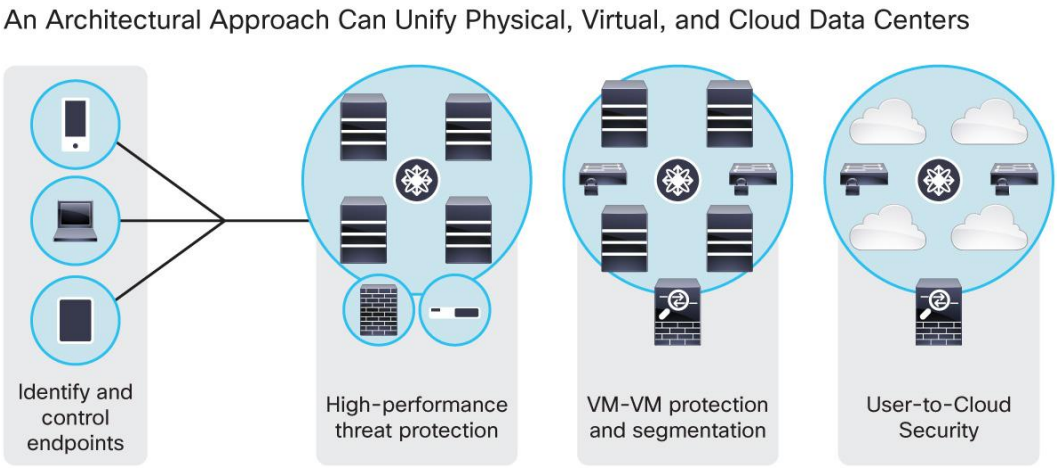
[2] Andi Mann, Kurt Milne, and Jeanne Morain, "Calculating the Cost Advantages of Private Cloud"; http://searchcloudcomputing.techtarget.com/feature/Calculating-the-cost-advantages-of-private-cloud, April 2011.

Loss of Control and Visibility

- **System complexity and multiple teams:** Many companies feel there is a loss of visibility as you move to the cloud. Traditional firewalls and intrusion prevention systems outside the virtual zones don't see traffic between virtual machines. In many cloud deployment scenarios, customers have no knowledge of the underlying security products because they are being managed by an outside source.
- **Compliance:** Cloud infrastructures must be compliant with industry standards, customer standards, and regulatory standards. They should support visibility and auditing capabilities. Industries with substantial compliance regulations such as healthcare, finance, and government must have an audit trail.

Because of their concerns about the loss of control and visibility, many enterprises believe the move to the private cloud is the better choice. That said, security issues - including access to data and application security - are still legitimate concerns in private cloud deployments. Figure 1 summarizes the benefits of an architectural approach.

Figure 1. Benefits of an Architectural Approach to Private Cloud Deployment



Private Cloud Architecture Considerations

From an architectural standpoint, the main components of private clouds are the underlying infrastructure, various service components, and certain pervasive functions such as security and resiliency. Furthermore, cloud security has its own architectural structure. Some key considerations are:

- **Logical separation:** An important benefit of cloud computing is "elastic" computing capabilities, meaning that computing power can be ramped up or dialed down rapidly based on demand. To support such a dynamic business-computing model, security should be provisioned in a similar manner. Static and physically oriented security configurations such as VLAN-based security are labor-intensive and can hardly keep up with the fast pace. New approaches are needed to achieve logical separation so that dynamic and shared environments with multiple tenants can be secured.
- **Policy consistency:** An overarching and consistent policy framework is critical for successful cloud security implementation. For example, an excellent design to achieve reliable and dynamic logical separation is to apply zone-based and policy-driven security enforcement. A zone is a group of attributes that may include traditional networking parameters such as IP addresses, network protocols, and port numbers. The zone may also contain information such as virtual machine (VM) and custom attributes. Approaches such as this help ensure policy consistency in a dynamic cloud environment where VMs typically move around between physical servers.

- **Automation:** A core tenet of the cloud-computing business model is that it allows for fast, efficient, and repeatable tasks. It lets end users take on tasks that IT staff performed previously by transferring these tasks to a self-service model. A centralized security policy framework with automated push mechanisms can greatly improve business efficiencies by mapping a security policy to a technical implementation.
- **Scalability and performance:** Closely tied to automation, scalability and performance are requirements for cloud security because of the potentially massive workloads and stringent security requirements involved. Innovative technologies that can help boost performance while maintaining a high security standard are critical to cloud security implementations.
- **Authentication and access control:** As previously discussed, access control to the private cloud depends on context-aware attributes and the identity, device, and location of the user. To authenticate and provide secure access to the private cloud environment from multiple devices and locations, it's critical to implement security from within the network and to have multiple enforcement points (such as the firewall, IPS, and VPN).

Cisco Secure Data Center Solution for the Private Cloud

Cisco's Secure Data Center solution for private cloud focuses on a secure cloud infrastructure. The Cisco product portfolio includes the following security components:

- Cisco ASA 5585-X Adaptive Security Appliance or the Cisco Catalyst® 6500 Series ASA Services Module
- Cisco Adaptive Security Appliance (ASA) Software Release 9.0
- Cisco IPS 4500 Series Sensors or IPS blade for the ASA 5585-X
- Cisco TrustSec® Security Group Access
- Cisco Security Manager 4.3
- Cisco Nexus® 1000V Series Switches
- Cisco Virtual Security Gateway (VSG)
- Cisco ASA 1000V Cloud Firewall
- Cisco Virtual Network Management Center (VNMC)

The Cisco ASA 5585-X appliance is uniquely positioned to provide high-performance security to protect the new virtualized data center and extended cloud with firewall and intrusion prevention (IPS) capabilities. Deploying the ASA 5585- X at the cloud data center distribution layer provides strong protection for high-valued cloud resources and services. The ASA 5585-X supports advanced virtual data center technologies, such as Cisco virtual port channel (vPC), Cisco Catalyst 6500 Virtual Switching System (VSS), and Cisco Nexus 7000 Series virtual device contexts (VDCs). These technologies enable high scalability and performance for cloud environments. Furthermore, the ASA 5585-X supports multiple security contexts that enable efficient logical separation to keep all customer traffic separate and secure in a multitenant environment.

The Cisco ASA 5585-X appliance features MultiScale™ performance, which provides rapid connections per second, an abundance of concurrent sessions, and accelerated throughput, and enables multiple security services for exceptional flexibility. The ASA 5585-X can offer up to 20 Gbps of real-world HTTP traffic and up to 35 Gbps of large packet traffic. It supports up to 350,000 connections per second and a total of up to two million simultaneous connections initially.

The Cisco ASA Services Module provides similar high performance, but is deployed as a plug-in module for Cisco Catalyst 6500 Series Switches.

Cisco ASA Software Release 9.0 delivers enterprise-class security capabilities for ASA devices in a variety of form factors, including a wide range of standalone appliances, hardware blades that integrate with the organization's existing network infrastructure, and software that can secure and protect public and private clouds. Major new features in Release 9.0 include clustering; integration with Cisco Cloud Web Security (formerly ScanSafe), which allows enterprises to enforce granular web access and web application policy while providing protection from viruses and malware; and Cisco TrustSec Security Group Tags (SGTs), which integrate security into the network fabric to extend the policy construct on the ASA platform

Cisco TrustSec Security Group Access classifies systems or users based on context as they connect. This innovative technology transforms the way organizations implement security policy across their data center infrastructure. Context-based classification propagates using SGTs to make intelligent policy-based forward or blocking decisions in the data center. In addition, TrustSec Security Group Access automates firewall rules and removes the management complexity in access control administration.

Cisco also provides the most widely deployed IPS technology in the market, offering a choice of dedicated IPS sensors or ASA firewall-integrated IPS services. The Cisco IPS 4500 Series Sensors or the IPS blade for the ASA 5585-X helps to ensure protection and availability for critical applications and infrastructure at data center speed, supporting over 100,000 connections/second. An expandable 10 Gigabit Ethernet chassis in a compact 2RU form factor supports scale and investment protection while meeting "green data center" goals.

The IPS 4500 protects infrastructure and applications from advanced persistent threats (APTs) and other sophisticated attacks using state-of-the-art technologies such as threat intelligence, passive OS fingerprinting, and reputation along with contextual analysis to deliver superior security protection. Backed by Cisco Security Intelligence Operations (SIO), Cisco IPSs gain visibility generated by hundreds of security parameters, millions of detection rules, and 8 TB of threat telemetry per day from market-leading email, web, firewall, IPS, and endpoint clients.

Cisco Security Manager 4.3 is a comprehensive management solution that enables consistent policy enforcement, rapid troubleshooting of security events, and summarized reports across the security deployment. It manages the Cisco security environment, provides visibility across the deployment, and enables information sharing with other essential network services. It also maximizes operational efficiency with a powerful suite of automated capabilities. Cisco Security Manager manages the Cisco security environment for Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IPS 4500 Series Sensor Appliances, the Cisco AnyConnect® Secure Mobility Client, and Cisco secure routers.

The Cisco Virtual Security Gateway works with Cisco Nexus 1000V Series Switches to provide zone-based and policy-driven security at the virtual machine level, extending existing security policies into virtual and cloud environments. The Virtual Security Gateway provides secure segmentation to achieve logical separation at the VM level. Because the Virtual Security Gateway uses security-zone-based policy implementation rather than static IP addresses, it can consistently enforce security policies even as VMs move from one physical host to another. This support of VM mobility is critical to ensure policy consistency in an automated cloud environment where workloads can be processed anywhere in the cloud.

The Cisco Virtual Security Gateway also provides auditing and visibility capabilities at the tenant level, which is critical for compliance purposes. The Cisco Nexus 1000V adds additional security and monitoring capabilities at the access layer, including private VLANs, IP Source Guard, Dynamic Host Configuration Protocol (DHCP) snooping, Address Resolution Protocol (ARP) inspection, and NetFlow. The vPath intelligence embedded in a Cisco Nexus 1000V switch can also offload policy enforcement capabilities at the hypervisor layer from the Virtual Security Gateway, providing enhanced performance. Finally, a single Virtual Security Gateway can protect multiple physical hosts. Such flexibility greatly increases the scalability of Cisco cloud security and reduces the operational complexity associated with managing virtual firewalls on every physical host.

The Cisco ASA 1000V Cloud Firewall integrates with the Cisco Nexus 1000V Series virtual switch to help secure multitenant virtual and cloud environments at the tenant edge. The ASA 1000V acts as the default gateway, and provides security against network-based attacks. It is built using the ASA infrastructure and offers edge functionality including site-to-site VPN, Network Address Translation (NAT), DHCP, and inspections. A multitenant data center or private community cloud naturally requires complete isolation of application traffic between different tenants, applications, and user groups, depending on the policies that are in place.

Together, the Cisco Virtual Security Gateway and Cisco ASA 1000V provide end-to end security for multitenant private and public cloud deployments. To enforce granular security policies specific to individual virtual machines, the gateway and firewall tightly integrate with the Cisco Nexus 1000V Series virtual switch and the resident hypervisor in the virtualization layer of the server. As new virtual machines are instantiated or migrate between servers, the appropriate security policies for the virtual machine also migrate along with the virtual machine, providing all the necessary security services automatically. The Cisco Nexus 1000V Switch also provides service-chaining capabilities between the Virtual Security Gateway and the ASA 1000V.

The virtual firewall instances can be created and shared as demands and service loads require, for optimal resource utilization. Both the Cisco ASA 1000V and Cisco Virtual Security Gateway use the Cisco Nexus 1000V Series Switch's vPath traffic steering capability to steer traffic to appropriate networking services for policy enforcement. This approach enables a single instance of the ASA 1000V or Virtual Security Gateway to secure the VMs on multiple hosts, ensuring that the security infrastructure of the data center or cloud is scalable and can be easily managed. The number of instances of ASA 1000V and Virtual Security Gateway firewalls can grow according to need and a large number of policies specific to the various virtual applications can be enforced. This architecture helps to ensure resource optimization and cost savings for the end user.

Cisco's integrated solution is also built to scale across heterogeneous hypervisor environments. As the Cisco Nexus 1000V Switch scales across different types of hypervisors, the services that run on the Nexus 1000V, including the Virtual Security Gateway and ASA 1000V, also scale to secure these heterogeneous environments, so that purpose-built solutions for each type of hypervisor are not required.

The Virtual Security Gateway and the ASA 1000V are managed through the Cisco Virtual Network Management Center, which supports both a built-in GUI and transparent operation management through an XML API. This XML API enables programmatic integration with third-party management and orchestration tools, a capability that is critical to enabling cloud security service automation.

Altogether, Cisco's security portfolio solution enables in-depth cloud security for logical separation, policy consistency, automation, and access control in the cloud infrastructure. The Cisco solution helps secure multitenancy in private cloud environments and provides network traffic and activity visibility to help customers and service providers alike improve their cloud governance processes.

Summary

Organizations that have strong policy and compliance concerns are increasingly adopting private clouds to gain the benefits of cloud computing without the potential security risks. While a private cloud model sidesteps the security issues that arise in a public cloud environment, it still requires new security approaches to overcome the risks associated with shared resources and to enforce access control, and data confidentiality. Cisco's Secure Data Center solutions for the private cloud offer an approach that provides consistent policy framework and automation, scales, is virtualization-aware, and will enable organizations to successfully make this transition.

For More Information

Cisco Data Center Security

Cisco ASA 5585-X Appliance or Cisco Catalyst 6500 Series ASA Services Module

Cisco IPS 4500 Series Sensors or IPS blade for the ASA 5585-X

Cisco TrustSec

Cisco Security Manager

Cisco Nexus 1000V Series Switches

Cisco Virtual Security Gateway

Cisco ASA 1000V Cloud Firewall

Cisco Virtual Network Management Center

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-714844-02 02/13