White Paper

Secure Separation in Cisco Unified Data Center Architecture

What You Will Learn

This document is written for technical professionals who want to increase the efficiency and flexibility of their data centers and are considering how to best implement security in a private cloud or multitenant data center environment, common for delivery of IT as a service (ITaaS).

Transforming the data center is a journey with predictable IT challenges along the way. Security, and its integration into the data center infrastructure, is a challenge often faced by IT departments as they balance the transition from dedicated infrastructure per application to a shared model. To address these challenges, the Cisco® Unified Data Center platform delivers three technology pillars: Cisco Unified Computing, Unified Fabric, and Unified Management. This document focuses primarily on the features, capabilities, and products of the Cisco Unified Fabric and their use in building a secure network. After reading this document, you will have an understanding of secure separation as a concept. You will also be aware of factors to consider in deploying a secure multitentent data center.

Introduction

Companies today are feeling increasing pressure to deliver cost-effective and efficient services that are responsive to current and future business needs. From an IT perspective, such services include initiatives to simplify IT operations by moving away from underutilized traditional systems through consolidation, unification of platforms, virtualization, and automation of the IT infrastructure. However, these same initiatives also must help make IT more nimble, allowing the business to launch new applications and services more quickly. To attain these goals, an architecture evolution has begun that is transforming the traditional data center to a virtualized environment and, eventually, to a public, private, or hybrid cloud environment.

This trend is also creating new security challenges that should be addressed prior to migration to a cloud environment. These challenges are complex because they involve both technology issues and significant process changes due to new business computing models. As companies transition and evolve their infrastructure, they need to fully understand how security fits into these new architectures and adopt new security tools to help ensure that the transfer of information is protected throughout their environments. Companies also must help ensure that new security policies and technologies do not limit the scalability and performance of their new virtualized data center environments.

An extremely important security requirement for companies and service providers that host segmented, shared, virtual environments is secure separation. Secure separation, or multitenancy, is the separation of workloads and virtual machines to meet customer or tenant separation, security, compliance, and service-level agreement (SLA) requirements while using a common computing, storage, and networking infrastructure. Today's consolidated data centers and clouds have disparate user groups with needs that range from simple segmentation to complete separation of network traffic and strict access control policies, even though they are sharing the same physical servers and network infrastructure.

As enterprises migrate to private cloud environments, thereby virtualizing the underlying infrastructure that was formally physically dedicated on a per-tenant or per-department basis, these enterprises must help ensure that they maintain current levels of security, compliance, and quality of service (QoS).

This document examines varying degrees of secure separation through use cases. It shows how, as an organization grows and evolves from physical to virtual to cloud computing environments, different levels of secure separation are necessary. It also presents a use case with the highest levels of secure separation. This document discusses the different levels of secure separation needed as a company experiences the following growth cycles, starting with dedicated infrastructure and moving to a private cloud environment:

1. Organization with a single shared infrastructure and multiple applications that requires secure separation between applications and departments
   - Dedicated infrastructure for mission-critical applications; very common requirement for applications such as those from Oracle and SAP
2. Larger organization with shared infrastructure and secure separation requirements
   - Multiple departments with different QoS requirements based on SLAs or business priorities (for example, customer relationship management [CRM] traffic has a better SLA guarantee than video traffic)
   - Basic premise of virtualization: shared resources with virtual containers for various software applications
3. Single organization that has grown into multiple organizations, needing more separation and adding virtualization, and offering private cloud as well as cloud resources to integrate an acquisition
   - Need to meet legal separation requirements, helping ensure that traffic does not overlap: for example, a group that manages credit card information should be secured differently than the engineering network
   - Critical need for separation of individual virtual environments
4. SLA-assured cases such as healthcare organizations, in which IT functions as a service provider with associated guarantees
   - Creation of boundaries and assurance of separation
   - Orchestration and simplification

Designing a Security Model for Secure Separation

One of IT's greatest concerns in the data center is security. Customers are seeking to protect high-value targets, enable service delivery, help ensure availability, and comply with regulatory requirements. Customers also require high-performance data center security that can handle massive workloads, many different types of data, and transaction-heavy network traffic. IT needs to keep the following common security concerns and concepts in mind when investigating a move to a multitenant or private cloud environment:

Multitenancy and segmentation

- Multitenancy: Whereas small, distributed data centers host a small number of applications or support a single organization, today's consolidated data centers and clouds often 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. These same requirements apply to private virtual data centers and private clouds, in which internal tenants require separation.

- Segmentation: Large enterprises may have thousands of applications, which can be segmented by business unit, importance (mission critical or not mission critical), function, etc. Each of these segments must be protected with consistent security controls that span both the physical network and the cloud to prevent loss from external and internal threats. As an organization becomes more segmented, virtualizes, and moves applications to the cloud, the network becomes more sophisticated and more complex, especially as automation and orchestration are added.

Secure application access

- Identity and authorization: In a world of increasing mobility, unsecured devices, and increasingly sophisticated threats, the network must take over more of the security policy enforcement responsibilities from the applications. Therefore, the network infrastructure is performing more user authentication and access policy authorization enforcement, taking over this activity from the application endpoints as networks become more context and application aware. The network security infrastructure is increasingly required to enforce identity and role-based policies, as well as 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 application in the transaction.
- Local and remote access: Access can also depend on context-specific attributes besides 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 and control traffic 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 range of mission-critical commercial and highly customized applications. The data in those applications is a high-value target for attackers, yet access to that data is what fuels the productivity and success of the enterprise.

Visibility and compliance in the cloud

- System complexity and multiple teams: Many companies believe that they lose visibility when they move to a public or hybrid cloud. Traditional firewalls and IPSs outside the virtual zones do not see the traffic between virtual machines. In many public cloud scenarios, customers have no knowledge at all of the underlying security products because the cloud environment is being managed by an outside source.
- Compliance: Cloud infrastructure must comply with industry standards, customer standards, and regulatory standards. It should support visibility and auditing capabilities. Industries with substantial compliance regulations such as healthcare, finance, and government fear a lack of an audit trail.
- Private or public cloud: Due to the loss of control and visibility, many enterprises believe that a move to a private cloud, rather than a public cloud, is a better choice. However, even in a private cloud, information security concerns and needs still exist, and data and application access must be secure. Security is, in fact, integrated throughout the private cloud computing architecture.

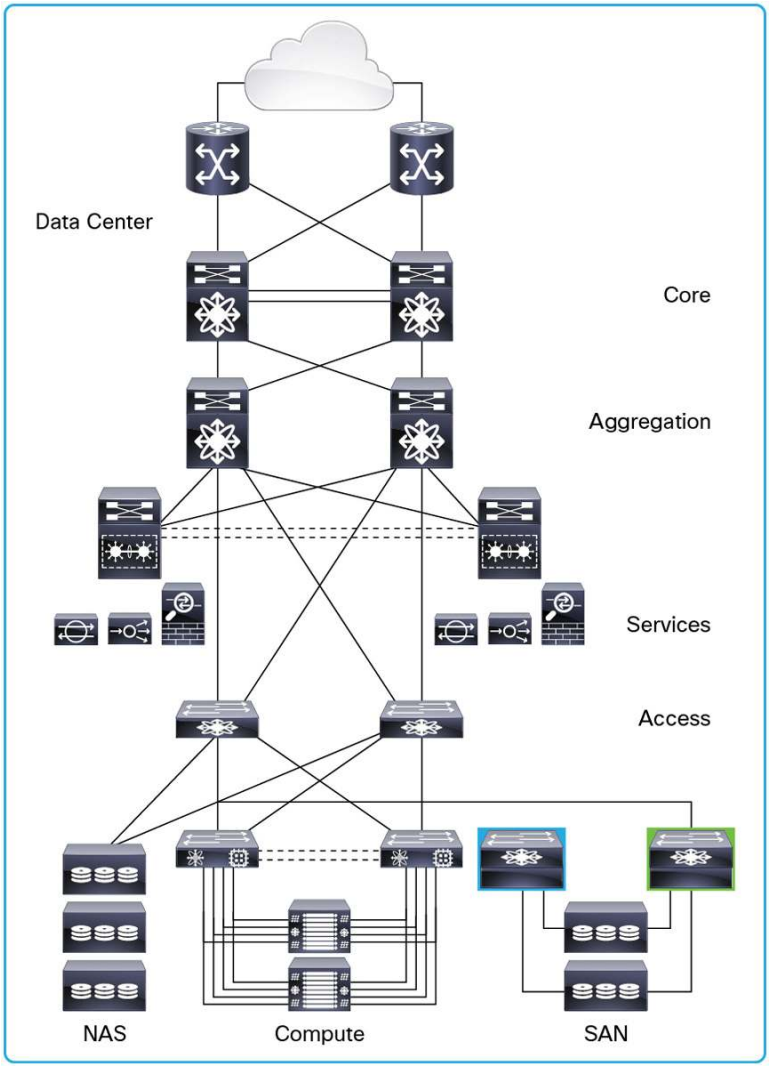
Secure-Separation Use Cases

Secure separation in a multitenant data center infrastructure is the underlying security technology that provides the capability to create virtual containers within a data center architecture. Secure separation helps ensure the separation of workloads and virtual machines to meet customer separation, security, compliance, and SLA requirements on the basis of the service being delivered.

The five use cases discussed here demonstrate different degrees of secure separation in a data center environment as an organization evolves from a traditional level of secure separation in use case 1 and adds multitenant security and isolation as warranted. As these uses cases show, as the organization's security requirements change as a result of events such as acquisition, growth, the addition of new applications, and new compliance needs, Cisco can add and products and features to the existing architecture to meet the new requirements.

These use cases are based on a traditional hierarchical data center foundation, depicted in Figure 1. Hierarchical designs have commonly been used in networking to achieve scalability and high availability, and they are used similarly in the Cisco Unified Data Center to create a robust network framework. In a hierarchical design, the Cisco network is organized into core, aggregation, and access layers.

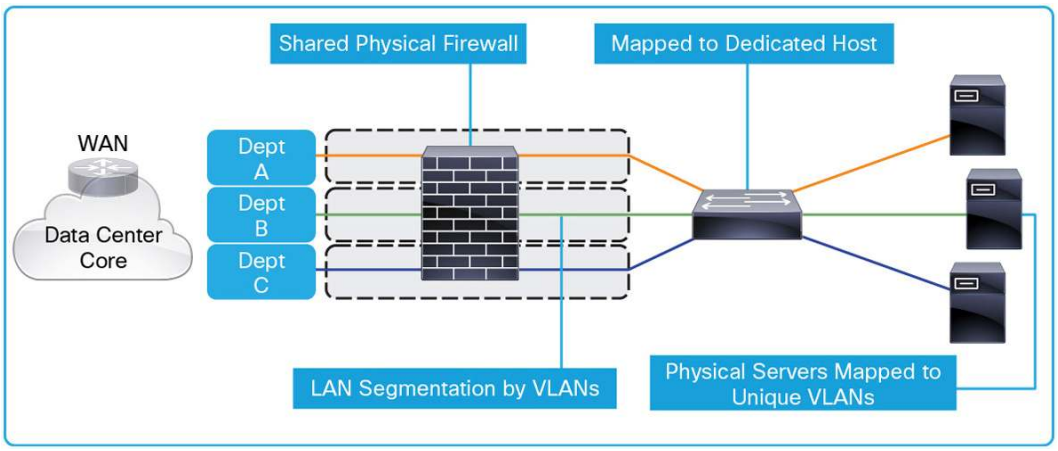
Figure 1. Hierarchical Network Design



Use Case 1: Organization with a Single Shared Infrastructure and Multiple Applications That Requires Secure Separation Between Applications and Departments

Figure 2 shows use case 1.

Figure 2. Use Case 1



Organization Security Requirements

- Departments A, B, and C require secure separation and individual access to applications for security and compliance.
- The organization requires some elements of secure physical separation and some elements of secure virtual separation.

Use Case 1 Products

- Cisco ASA 5500 Series Adaptive Security Appliances physical firewall, Cisco Nexus® switching infrastructure, and physical hosts.

Internet Edge

Policy is implemented at the WAN edge, which is the common infrastructure Layer 3 perimeter that provides access control for the corporate network and the data center. These are the main features and capabilities often enabled at that level:

- Infrastructure security rule sets are implemented through router access control lists (ACLs).
- A network-based firewall is inserted between the physical network and multiple virtual networks.
- Context-based virtualization is used.
- Topology, provisioning, and monitoring is isolated per tenant.

Shared Physical Firewall

The Cisco ASA 5500 Series appliance provides a single physical firewall that is shared by tenants A, B, and C and which serves to filter external traffic while providing VPN access protection and threat mitigation. VLANs provide segmentation and are mapped to the security domains of each tenant.

Tenant Containers

Cisco Nexus Family switches with VLANs provide isolation between tenant containers A, B, and C. VLANs provide the capability to securely partition a physical network in software to provide optimal asset utilization.

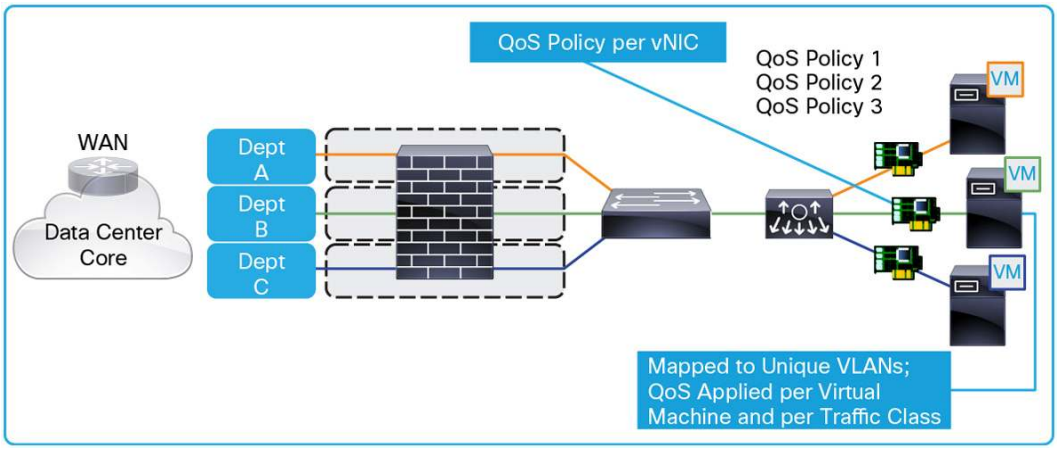
Hosts

Dedicated physical servers complement this model, further implementing physical separation of traffic from the hosts to each tenant. Physical servers are mapped to specific applications, which are mapped to a set of VLAN and security policies.

Use Case 2: Organization with a Single Shared Infrastructure with Multiple Applications That Require Elements of Secure Physical Separation and Elements of Secure Virtual Separation

Figure 3 shows use case 2.

Figure 3. Use Case 2



Organization Security Requirements

- The organization has multiple departments with different QoS requirements.
- The basic premise of virtualization is shared resources with virtual containers for various software applications.
- The organization needs to help ensure separation of workloads and virtual machines to meet customer separation, security, compliance, and SLA requirements.

Products Added to Use Case 1

- Cisco Nexus 1000V Switch, virtualization hypervisor and virtual machines on physical hosts, and virtual network interface cards (vNICs; for virtual Ethernet on the Cisco Nexus 1000V).

Hosts

Virtualization is added to hosts to create secure containers that extend from the host across the network on a per-tenant basis.

Device virtualization in the form of a Cisco Nexus 1000V virtual switch is used to segment traffic flows at a per-virtual machine level and to provide insertion points for application and security services.

Cisco Nexus 1000V and Cisco VN-Link technology provide visibility into the individual virtual machines, and policies can now be configured per virtual machine and enforced on the Cisco Nexus 1000V.

Virtual machine traffic can be sent to physical appliances, for example, using VLANs, where network services can be applied. Virtual contexts can be used to provide multitenancy.

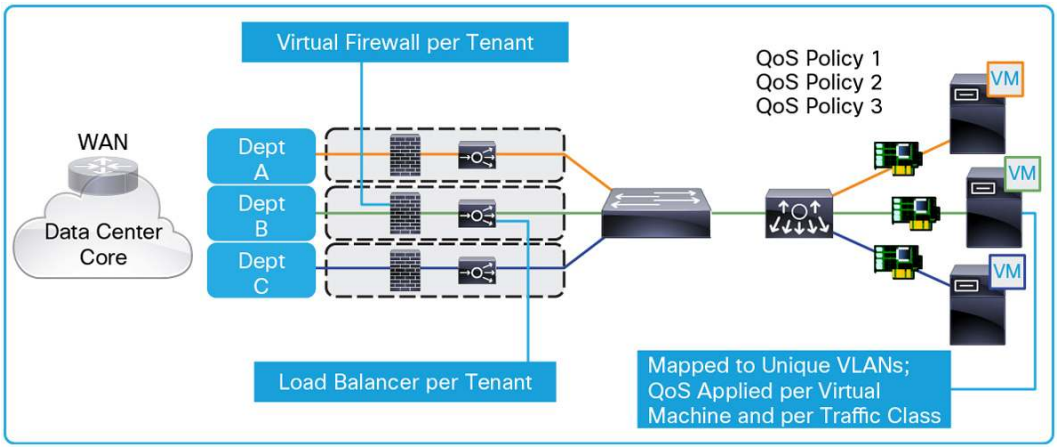
QoS Policy per Tenant

The Cisco Nexus 1000V provides per-virtual machine visibility, policy, and monitoring capabilities. Class-based weighted fair queuing and low-latency queuing are also supported on the Cisco Nexus 1000V, so QoS policies can be applied on a high-touch basis per tenant virtual machine (that is, on a per-vNIC basis) for each traffic class. Within the remaining Cisco Nexus switching and service nodes, the classifications and markings set at the Cisco Nexus 1000V are matched and queued appropriately.

Use Case 3: Single Organization That Has Grown into Multiple Organizations, Needing More Separation and Adding Virtualization, and Offering Private Cloud as Well as Cloud Resources to Integrate an Acquisition

Figure 4 shows use case 3.

Figure 4. Use Case 3



Organization Security Requirements

- The organization requires differentiated QoS levels for each application according to the use case.
- Additional isolation per tenant (firewalls and services) is needed to help ensure that legal separation requirements are met, helping ensure that traffic does not overlap.
- Separation between individual virtual environments is critical.

Products Added to Use Case 2

- Virtual firewall and load balancer per tenant.

Dedicated Virtual Contexts on a Per-Tenant Basis

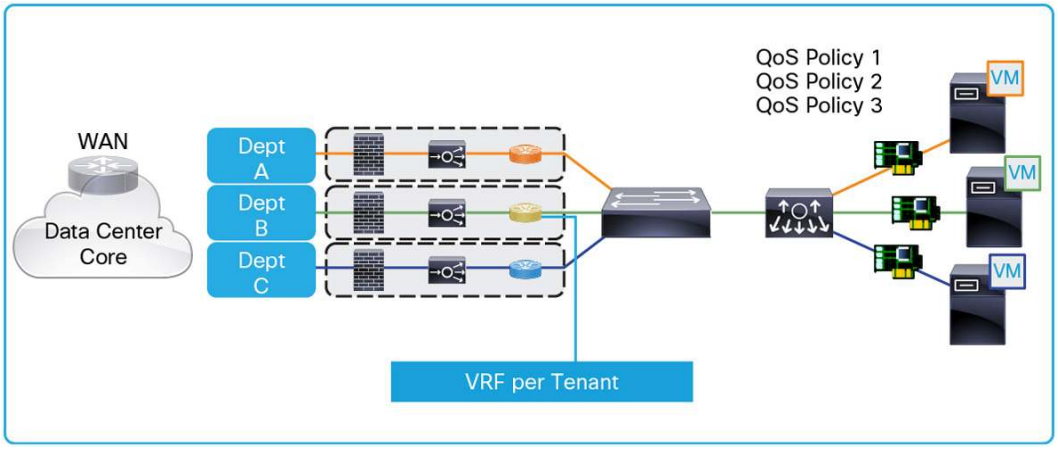
- Virtualization is used in service nodes.
- Firewall and load-balancing services are dedicated logically on a per-tenant basis.

- Cisco Application Control Engine (ACE) provides virtual contexts (virtualization is used on the physical service nodes), which are dedicated on a per-tenant basis to isolate traffic that needs to traverse the service nodes.
- The Cisco Nexus 1000V logically segments the firewall by tenant.

Use Case 4: SLA-Assured Cases Such as Healthcare Organizations, Which Require the Highest Degree of Tenant Separation and Isolation to Meet Compliance Requirements

Figure 5 shows use case 4.

Figure 5. Use Case 4



Organization Security Requirements

- The organization requires differentiated QoS levels for each application according to use case.
- For example, a hospital use case would help ensure that the customer meets U.S Health Insurance Portability and Accountability Act (HIPPA) compliance regulations.

Products Added to Use Case 2

- Dedicated virtual routing and forwarding (VRF) per tenant.

Virtual Routing and Forwarding

Some organizations require even more stringent security. This additional security often requires the creation of an overlay network that is securely separated from everything else. One way to provide this additional security is to use the VRF feature on the Cisco Nexus Family switches. The addition of a dedicated per-tenant VRF instance provides isolation of back-end application hosts (for example, tier 2 and 3 application and database servers, or entire applications).

VRF allows multiple instances of a routing table to coexist in the same router. Because the routing instances are independent, they play a crucial role in end-to-end separation of tenant traffic flows in a multitenant environment.

A global VRF instance is applied, and this is where shared resources and virtual machines can be placed. Shared resources can include a DMZ (with proxy servers, IPS, and a server-load balancing [SLB] farm for SSL offload processing).

Additional firewall zoning can be created through insertion of Cisco Virtual Security Gateway VSG virtual firewalls both in the common front-end zone and on a per-tenant basis in the unique back-end zones, for east-west zoning (providing more comprehensive support for N-tier application security and separation requirements).

Cisco Data Center Security Advantages

Cisco data center security enables an environment that is open to a wide range of business applications to support new business initiatives with policy controls. Pervasive Cisco data center security creates a personalized and unique end-user experience. Cisco data center security is also versatile and efficient, helping organizations achieve fast service delivery and operational excellence. With Cisco data center security, you can:

- Defend data center availability with threat defenses
- Secure data center services with application and content security
- Prevent business loss with secure access
- Meet compliance requirements with policy controls in both physical and virtual environments

Cisco data center security provides the following advantages:

- Cisco has the necessary technology know-how and a strong customer commitment.
- The Cisco security portfolio has the depth and breadth needed to address customer data center security challengers.
- Cisco innovations and architecture and Cisco Validated Designs support your deployment and maintenance efforts to help you achieve operational excellence and lower total cost of ownership (TCO).

Cisco Validated Design for Virtualized Multiservice Data Center

At Cisco, intensive testing is performed to help ensure design reliability and stability to meet your needs for a secure data center, secure virtual data center, and secure private cloud in a virtual environment.

The Cisco Virtualized Multiservice Data Center (VMDC) secures the unified data center that hosts mission-critical applications and sensitive data. The Cisco Unified Data Center changes the economics of the data center by unifying computing, storage, networking, virtualization, and management into a single, fabric-based platform, designed to increase operating efficiency, simplify IT operations, and provide business agility. Unlike other solutions, which add layers of management software to achieve integration, the Cisco Unified Data Center is specifically designed for virtualization and automation and enables on-demand provisioning from shared pools of infrastructure across physical and virtual environments. This approach allows IT to move from being a cost center to providing IT services that create competitive advantage.

Tightly integrated with the Cisco Unified Data Center are security controls provided by a market-leading firewall, VPN, hardware-accelerated IPS, and appliances and applications for the virtual environment. The secure Cisco VMDC Validated Design enables a transparent network flow from the physical to the virtual network, enabling agile operations and simpler management. It can create multiple security zones that logically separate tenant resources from one another in the virtual network and allow fault-tolerant virtual machine movement. Edge security protects the data center from external threats and offers secure contextual access to data center resources. The Cisco VMDC environment is intuitive, powerful, and secure, providing superior real-time protection for critical information assets using innovative IPS with global correlation, firewalls and web application firewalls (WAFs), and VPN technology.

As customers move to multitenant environments, organizations must address additional requirements, including:

- Simplified deployment and scaling of computing resources and secure virtual machine instantiation and operation
- Virtual machine awareness to support workload separation by trust level and logical group
- Secure self-service virtual machine requisition tools to enable customers to instantiate new virtual machines for temporary or permanent workloads as well as for development and testing
- Compliance templates and policy automation tools to couple security policy with the network orchestration

Cisco can help meet these additional requirements with zone role-based policy through virtual management and virtual gateways, secure transparent links for virtual machine mobility, and secure automation through additional validated designs that provide templates for compliance and policy.

Multilayer End-to-End Security with Cisco VMDC

Successful deployment of cloud architectures depends on complete end-to-end security of both the data center infrastructure and the virtualized environments that host the cloud consumer's application and service loads. The Cisco VMDC architecture addresses the security challenges by providing a complete framework for end-to-end security at multiple layers of the network.

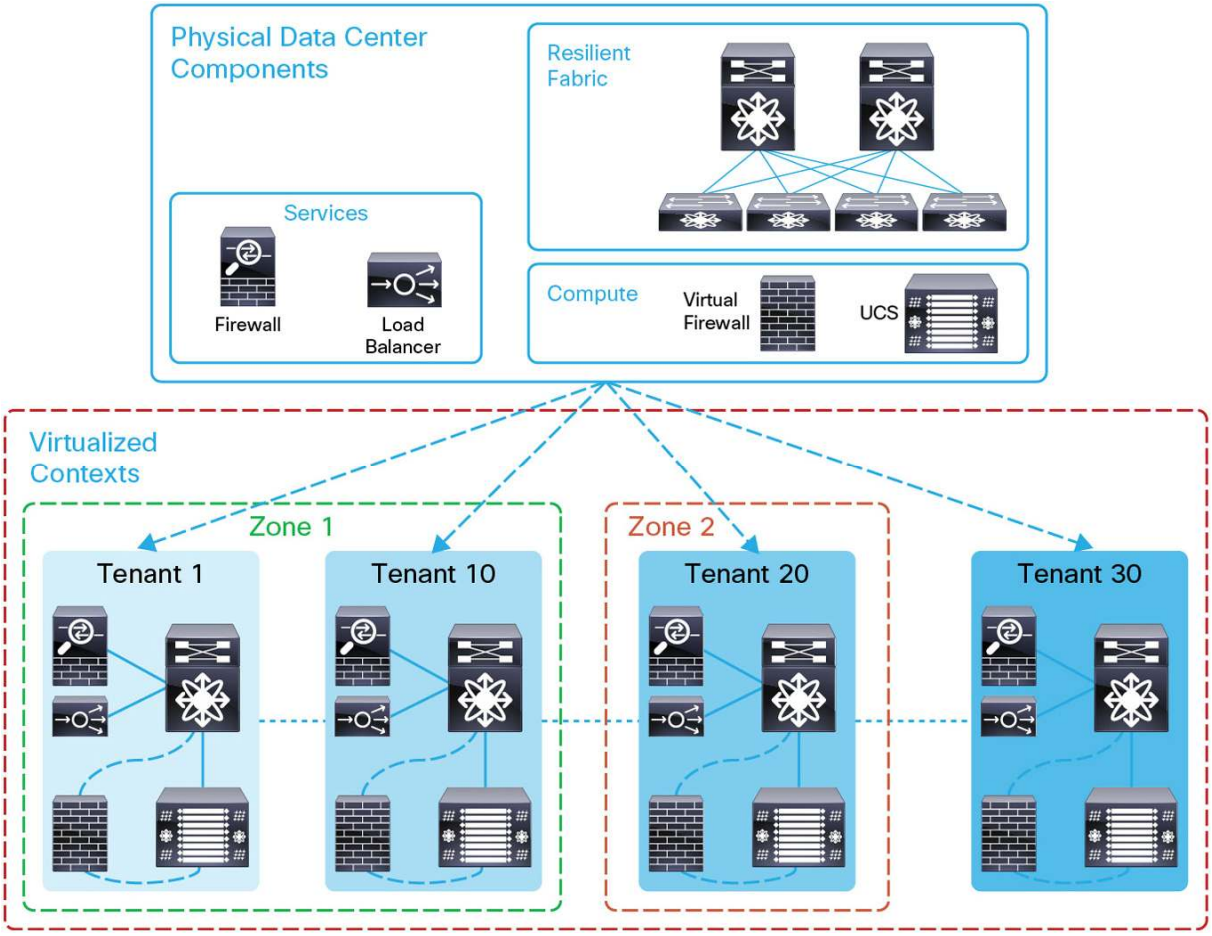
A proper security approach requires deployment of a number of complementary security services at appropriate points in the data center network. These data center security requirements include:

- Defending the data center from unauthorized users and outside attacks
- Preventing intrusion and data containing malware
- Defending the tenant edge with a proven firewall to secure both virtual and cloud infrastructure
- Assigning virtual machines to segmented trust zones within the virtual network and enforcing access policies at the virtual server level
- Providing centralized multitenant policy management
- Supporting virtual machine mobility
- Securing access to the virtualized data center and applications
- Providing a security solution that scales with the rest of the cloud-ready infrastructure
- Separating security, network, and server administrator duties

The Cisco VMDC architecture uses Cisco's physical and virtual security portfolio, which includes the Cisco ASA 5585-X Adaptive Security Appliance, Cisco ASA 1000V Cloud Firewall, Cisco VSG, Cisco Nexus 1000V Series Switches, and Cisco Virtual Network Management Center (VNMC) for consistent physical and tenant edge and intratenant security and policy management. Cisco vPath through the Cisco Nexus 1000V Series Switch improves security agility and efficiency, and dynamic context-aware multitenant management security is available using Cisco VNMC.

For multitenancy, a dedicated infrastructure traditionally is deployed for each tenant that is hosted. However, this approach does not scale well because of cost, complexity to manage, and inefficient use of resources. In Cisco VMDC, multiple tenants in a common infrastructure can efficiently use shared resources to achieve lower costs. Each tenant may require path isolation for security and privacy to separate the tenant from others sharing the common infrastructure. Logical separation or virtualization, which is a fundamental concept for multitenancy is achieved in the Cisco VMDC architecture at the networking, computing, and storage levels (Figure 7).

Figure 6. Multitenancy Design



Conclusion

Cisco secure data center solutions for the private cloud help ensure secure multitenancy in private cloud environments and provide visibility into network traffic and activity to help customers maintain their cloud governance processes. As customers embark on their cloud journey, Cisco security helps them reduce their risks with consistent policies and enforcement, greater scalability, and improved performance. Cisco security, together with the Cisco Unified Data Center, helps remove the barriers cloud adoption regardless of whether you are updating your data center or building a new one, helping customers achieve the economies of scale and efficiency of cloud computing in a secure way.

For More Information

- Cisco data center security: http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns224/ns376/index.html
- Cisco ASA 5585-X Appliance and Cisco Catalyst® 6500 Series ASA Services Module: http://www.cisco.com/en/US/partner/products/ps11621/index.html
- Cisco IPS 4500 Series Sensors and Cisco ASA 5585-X IPS Security Services Processor: http://www.cisco.com/go/ips
- Cisco Nexus 1000V Series Switches: http://www.cisco.com/en/US/partner/products/ps9902/index.html
- Cisco VSG: http://www.cisco.com/en/US/partner/products/ps11208/index.html
- Cisco ASA 1000V Cloud Firewall: http://www.cisco.com/en/US/partner/products/ps12233/index.html
- Cisco VNMC: http://www.cisco.com/en/US/partner/products/ps11213/index.html
- Cisco Unified Data Center: http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns224/architecture.html
- Cisco VMDC Validated Design: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

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 C11-722425-00 12/12