Cisco VMDC Cloud Security 1.0 Design Guide

December 3, 2014

Building Architectures to Solve Business Problems

Cisco VMDC Cloud Security 1.0 Design Guide

Service Provider Segment

CONTENTS

Preface

Rapid technological changes and evolving business requirements continually challenge organizations to protect their assets. While constant change in the business landscape drives the adoption of new technologies in IT networks, organizations find it increasingly difficult to address new and more sophisticated attacks that threaten corporate assets and disrupt business operations.

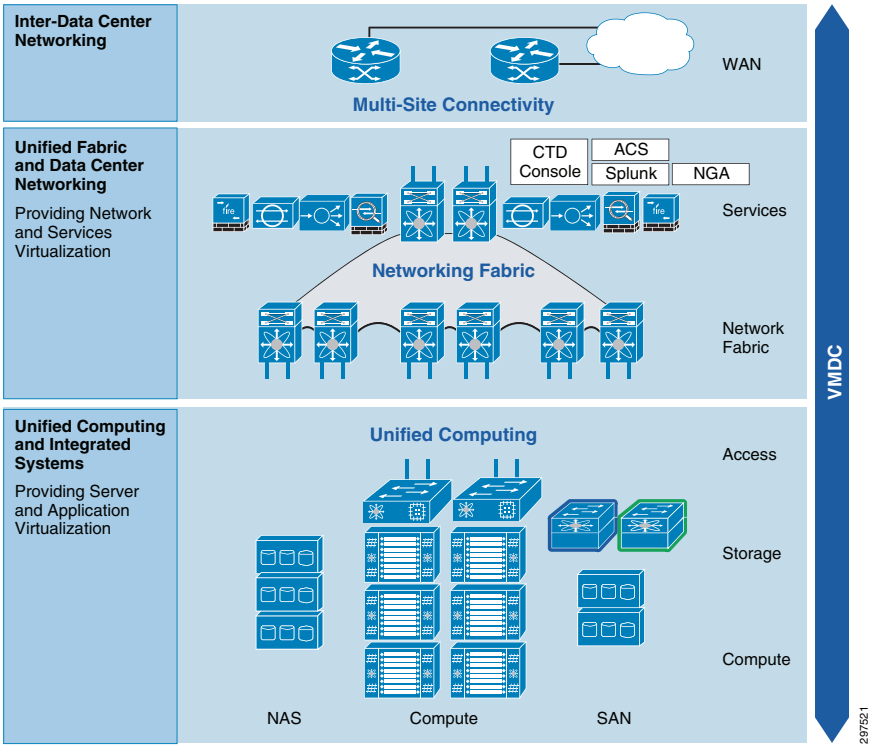
Localized security policies and devices at network perimeters can no longer safeguard corporate assets nor ensure operational continuity. Today, secure corporate networks require multiple layers of protection and implementation of a unified, system-wide, security strategy. The current Internet security landscape emphasizes the need for end-to-end security architectures, along with design and implementation guidelines for building secure and resilient network infrastructures.

In particular, data centers need secure infrastructures. In any organization, a typical data center houses the most critical and valuable assets. This guide describes an architectural data center security framework, based on Cisco's Virtual Multiservice Data Center (VMDC) 2.3 architecture, specifically designed to work with the rest of organizations' network security infrastructures.

This guide is written for network and security engineers to help them to design, implement, and operate secure network infrastructures that address today's challenging business environments.

Cisco VMDC Cloud Security Release 1.0 is a reference architecture providing design and implementation guidance for cloud deployments. Numerous service providers and enterprises have implemented multiple VMDC versions in private, public, and hybrid cloud deployments. VMDC Cloud Security 1.0 provides an end-to-end validated system that integrates a variety of Cisco and third-party products. Figure 1 shows the VMDC layers and major components.

Figure 1 VMDC Layers and Major Components



CHAPTER 1

Introduction

As service providers increasingly provide cloud-based services to enterprises and small businesses in virtual and multi-tenant environments, their security strategies must continually evolve to detect and mitigate emerging threats. In the VMDC reference architecture, physical and virtual infrastructure components such as networks (routers and switches), network-based services (firewalls and load balancers) - and computing and storage resources are shared among multiple tenants, creating shared multi-tenant environments.

Security is especially important in these environments because sharing physical and virtual resources increases the risk of tenants negatively impacting other tenants. Cloud deployment models must include critical regulatory compliance such as Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS).

The VMDC Cloud Security 1.0 solution enables customers to:

- Detect, analyze, and stop advanced malware and advanced persistent threats across the attack continuum.
- Consistently enforce policies across networks and accelerate threat detection and response.
- Access global intelligence using the right context to make informed decisions and take fast, appropriate action.
- Comply with security requirements for regulatory requisites such as FISMA, HIPAA, and PCI.
- Support secure access controls to prevent business losses.
- Secure data center services using application and content security.

Challenges

When deploying multi-tenant cloud data centers, Service providers are challenged to provide a secure, physical and virtual, environment for tenants. When onboarding tenants of different vertical segments such as financial, health care, or federal the service provider faces a bigger challenge in terms of meeting industry standards and legal compliance within their data center and services. The following sections highlight the key challenges the service provider may have.

Multi-Tenancy and Secure Segmentation

Service Providers (SPs) can use multi-tenant data centers to efficiently and economically provide cloud services using shared hardware and network infrastructures. For security, this approach requires complete separation of network traffic by tenant, along with strict access control policies, because multiple tenants share the same network infrastructure, and compute and storage resources. This is also true for large enterprises deploying private virtual data centers and private clouds, in which internal tenants require separation.

As SPs support multiple tenants in shared data centers, each tenant must be completely and securely segmented to protect them from external threats. Segmentation also provides threat boundaries that can confine threats. Data center tenants must be protected using consistent, ongoing security controls that span the physical and virtual infrastructures.

Secure Data Center Access

In multi-tenant environments with increased mobile device access and network and application virtualization, networks must perform increasing security enforcement in the face of new, highly sophisticated threats. Networks must do this before granting access to applications. As networks become more aware of context and applications, networks are taking over more user authentication and access policy authorization and enforcement tasks from applications.
The network security infrastructure is increasingly required to enforce identity 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 cannot be based simply on typical host source and destination addresses. Network and data center security must be based on the identities and roles of users, security policies, blacklisting, and application transactions.

In multi-tenant data centers, multiple tenants remotely access their applications, which typically share hardware and systems software with other tenants. The access can also depend on context-specific attributes other than identity, such as the type of device accessing the application, the location of the user, and the time of the request. Context-aware policies are increasingly the responsibility of data center firewall and intrusion prevention systems (IPS), intelligent log monitoring and detection. These capabilities must expand to detect and control traffic based on sophisticated policies and monitoring for the presence of malware, unauthorized access attempts, and attacks.

Industry Standards and Regulatory Compliance

Multi-tenant/multiservice data center deployments, which provide multiple cloud services to multiple enterprises, must ensure compliance with industry standards and regulatory requirements to support various different vertical industries, such as health care, finance, and defense. When SPs provide services and provision such tenants, they must comply with the industry standards and regulations, and must provide audit trails.

Solution Benefits

The VMDC Cloud Security Release 1.0 solution integrates Cisco and third-party products to deliver comprehensive, cohesive security frameworks for SPs and enterprises. The solution provides clear guidance for achieving compliance with industry standards and regulatory requirements in public,

private, and hybrid cloud deployments. The solution is built on a vPC-based VMDC release that is extensively validated for performance and scaling, and is widely deployed by enterprises and SPs worldwide. The following significant solution benefits are derived.

End-to-End Security

The numerous aspects of data center security are deployed among several network infrastructure elements. When deploying cloud data centers, service providers need to secure the data center end-to-end to protect their network environment and their customers data. VMDC Cloud Security 1.0 brings together many security devices in a cohesive manner with end-to-end validation to significantly reduce the implementation complexity enabling public cloud providers to improve time to market their services.

Integrates Additional Security Components with VMDC

VMDC provides a seamless approach and architecture for integration with various security elements, such as Cisco CTD, NGIPS, NGA, ACS, and Splunk. This significantly reduces implementation time and risks.

Addresses Key Cloud Provider Challenges

VMDC Cloud Security 1.0 validates use cases that address the key challenges that cloud providers face today, enabling them to achieve end-to-end security and data center compliance.

Provide Guidance for FISMA, HIPAA, and PCI DSS Compliance

VMDC Cloud Security 1.0 undergoes extensive third-party auditing to ensure that the security framework is compliance-ready. This potentially enables cloud providers to achieve compliances in an efficient and cost effective way. The solution provides detailed guidance and gap analysis to reduce the risk of compliance failure.

Audience

This guide document is intended for, but not limited to, security architects, system architects, network design engineers, system engineers, field consultants, Advanced Services specialists, and customers who want to deploy end-to-end security and achieve industry-standards and regulatory compliance in public and private cloud data center deployments.

- Readers should be familiar with the basic concepts of IP protocols, quality of service (QoS), High Availability, security technologies and requirements, and industry-standards and regulatory compliance acumen.
- Readers should understand general system requirements, along with enterprise and SP network and data center architecture.

Solution Scope

VMDC Cloud Security 1.0 provides a complete end-to-end data center security design with best practices for public and private cloud SPs, including:

- Policies, procedures, and best practices for an operational security framework to help mitigate risks, reduce deployment overhead and time to market, and assure cloud security in multi service data centers.
- Integrated, validated end-to-end security using elements in the VMDC reference architecture:
  - FirePOWER Next Generation Intrusion Protection System (NGIPS)
  - Cisco NetFlow Generation Appliance (NGA)
  - Cisco Secure Access Control System (ACS)
  - Cisco Cyber Threat Defense (CTD)
  - Splunk
- Performed Independent assessment and gap analysis of this design, with external auditors, with respect to PCI, FISMA, & HIPAA compliance frameworks.
- Enabling Service providers by leveraging security capabilities within the VMDC architecture, and refreshing prior VMDC cloud security related work where appropriate.
- Extending actionable recommendations to service providers seeking alignment with the aforementioned security compliance framework.

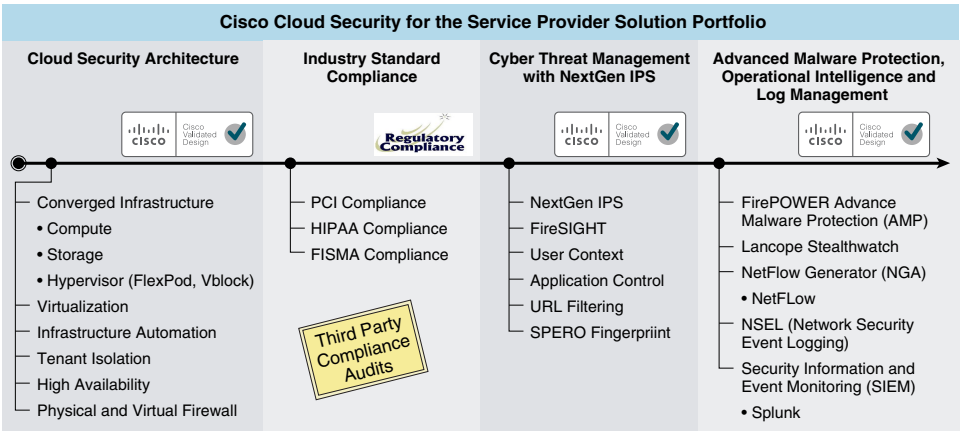
VMDC Cloud Security 1.0 is built on the VMDC 2.3 vPC-based Layer 3 (L3) hierarchical VRF-Lite DC design, supporting multi-tenancy, secure separation, differentiated service tiers, defense-in-depth, and high availability (HA).

This guide:

- Demonstrates recommended best practices and insertion strategies for a cohesive framework comprising key Cisco and third-party security elements.
- Provides comprehensive security guidance and an operational framework to support VMDC customer deployments.
- Provides detailed security guidance for using VMDC to support various security regulatory requirements; this solution release focuses FISMA, HIPAA, and PCI DSS.

Figure 1-1 shows the VMDC Cloud Security 1.0 solution portfolio.

Figure 1-1 VMDC Cloud Security 1.0 Solution Portfolio



Use Cases for End-to-End Secure Cloud Deployments

Cloud data center security is an important concern for both SPs and enterprises. SPs must protect their infrastructure, tenants, and services, and provide HA, and comply with industry standards and regulatory requirements. SPs must ensure that their security implementations do not adversely impact data center and network infrastructure performance.

Enterprises must trust that SPs deploy secure computing environments that isolate enterprise data and applications. Enterprises, like SPs, must comply with regulatory requirements.

This guide covers the following use cases:

- Compliance Fulfillment, page 1-5
- Identity and Access Management, page 1-6
- Next Generation Intrusion Prevention, page 1-6
- Network Visibility, Monitoring, and Threat Detection, page 1-6
- Real-Time Operational Intelligence—Event Monitoring and Logging, page 1-6
- Site-to-Site Virtual Private Networks, page 1-6

Compliance Fulfillment

Service providers when providing services from cloud to various different vertical markets such as card processing, Financial, Healthcare and Federal, they need to abide with the industry standard compliance. To achieve compliance on a complex data center cloud is a tedious, time consuming and costly, and without any proper guidance one can ran into failure and pay hefty fines for not getting compliant. Lack of compliance knowledge can cause major delays in service delivery, incurring huge opportunity costs in terms of time to market.

Note This release covers guidance on FISMA, HIPAA, and PCI DSS.

Identity and Access Management

Identity and access management is one of the issues service providers face in a multi-tenant environment where one or more tenants have access to various components of the data center. This creates a dire security threat if there is no centralized monitoring and management of access control.

Cisco Secure Access Control Server (ACS) provides a centralized highly scalable, policy-based network access and device access administration control platform that operates as a centralized RADIUS and TACACS+ server. It extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user-productivity gains.

Next Generation Intrusion Prevention

In multi-tenant cloud deployment virtualization and cloud computing introduce new security risks and challenges around new technologies and changing business processes. To succeed, organizations must address threat defense in depth to protect network from external and internal threats.

The Next Generation Cisco FirePOWER IPS provides threat detection capabilities that are currently required in multi-tenant cloud data centers deployments to mitigate new and emerging cyber threats.

Network Visibility, Monitoring, and Threat Detection

Network visibility in a multi-tenant data center with virtual environment is of primary concern for the service providers. They have to ensure that the same controls used in the physical world that are used in the virtual world. These controls need with the same consistent visibility and ability to see any and all traffic in and out of the data center.

This security architecture provides network visibility to monitor and detect the threat of malware spreading throughout a multi-tenant data center. Detecting threats and illegal activity within a network is an essential part of any security framework and architecture.

Real-Time Operational Intelligence—Event Monitoring and Logging

Event monitoring and logging is essential in any security framework and architecture. However, in a multi-tenant cloud data center deployments, it is difficult to identify security events in a timely manner and re-mediate them efficiently.

In VMDC Cloud Security 1.0, Splunk a technology partner virtual appliance is used that provide ability to monitor, search, analyze, visualize and act on the massive streams of machine data generated by the network and security appliances. It also perform monitoring of IT systems and infrastructure in real time to identify issues, problems and attacks before they impact your customers, services and revenue.

Site-to-Site Virtual Private Networks

Until recently, implementing site-to-site virtual private networks (VPNs) required additional hardware, such as an Aggregation Services Router (ASR) 1000 Series router, which increases OPEX and CAPEX. Now, Cisco Adaptive Security Appliance (ASA) products can implement site-to-site VPN inside ASA firewalls.

Incorporating site-to-site design inside ASA firewalls reduces network complexity for site-to-site VPN deployments on multi-tenant data centers significantly. It also reduces CAPEX.

Related Publications

The following design and implementation guides are available for respective iterative releases.

VMDC 2.x System Releases

In the data center portion of the architecture, VMDC 2.x designs centered on traditional hierarchical infrastructure models incorporating leading Cisco platforms and Layer 2 (L2) resilience technologies, such as virtual port channel (vPC), network containers and tenancy models of different sizes, and service profiles, along with network based services, orchestration, and automation capabilities for cloud providers and consumers.

- VMDC 2.3 Design Guide
- VMDC 2.3 Implementation Guide

VMDC 3.x System Releases

VMDC 3.x systems releases introduced Cisco FabricPath for intra-DC networks as an L2 alternative to hierarchical vPC-based designs. FabricPath eliminates the complexities of Spanning Tree Protocol (STP) to enable more extensible, flexible, and scalable L2 designs.

- VMDC 3.0.1 Design Guide
- VMDC 3.0.1 Implementation Guide

VMDC Virtual Services Architecture (VSA) System Releases

VMDC VSA is the first VMDC release dealing specifically with the transition to NFV (Network Function Virtualization) of IaaS network services in the data center. Such services comprise virtual routers, virtual firewalls, load balancers, network analysis and WAN optimization virtual appliances.

- VMDC VSA 1.0 Design Guide
- VMDC VSA 1.0 Implementation Guide

CHAPTER 2

Cloud Security Solution Overview

As more enterprises and small and medium (SMB) businesses move critical data and applications over to virtualized, multi-tenant systems in public and private clouds, cyber-criminals will aggressively attack potential security vulnerabilities. Security strategies and best practices must evolve to mitigate rapidly emerging, increasingly dangerous threats. The Cisco VMDC Cloud Security 1.0 solution protects against such threats, and provides a reference design for effectively and economically securing cloud-based physical and virtualized cloud data center deployments.

This design guide describes how to build security into cloud data center deployments. The VMDC Cloud Security 1.0 solution integrates additional security capabilities into data center design with minimal deployment risks, addresses governance and regulatory requirements, and provides improved technical controls to reduce security threats.

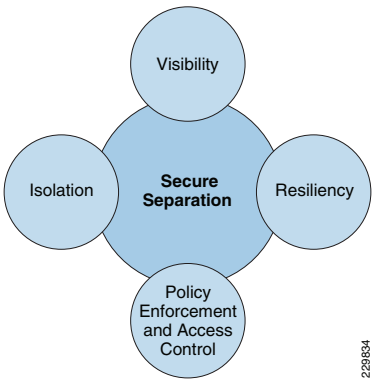
Providing end-to-end security for multi-tenant cloud data centers is a critical task that challenges service providers (SPs) and enterprises. However, deploying successful cloud data centers depends upon on end-to-end security in both data center infrastructures and the virtualized environments that host application and service loads for cloud consumers.

Security Architectural Principles

The primary security architectural principles for VMDC data center security are secure separation, visibility, isolation, resiliency, and policy enforcement as shown below:

Figure 2-1 shows the security principles incorporated in the security architecture.

Figure 2-1 Secure Separation Principles



Secure Separation

Secure separation describes the partitioning that prevents one tenant from having access to other tenants' environments and administrative features of the cloud infrastructure.

Isolation

Isolation provides a secure foundation for multi-tenant data centers and server farms. Depending on the design goals, isolation can be achieved using firewalls; access control lists (ACLs); virtual LANs (VLANs), Virtual Routing and Forwarding tables (VRFs), virtualization, storage networks, and physical separation. In addition, Intrusion Prevention appliances that can inspect traffic and detect security events on a per-VLAN basis can provide an additional level of threat isolation between different tenants. When combined, these can provide appropriate levels of security enforcement to server applications and services for multiple tenants.

Policy Enforcement and Access Control

Role Based access and authentication is an essential part of a comprehensive security framework. Obviously access to network devices and appliances needs to be regulated. If the infrastructure device access is compromised, the security and management of the entire network is at risk. Consequently, it is critical to establish the appropriate security measures and controls in order to prevent unauthorized access to infrastructure devices. Creating common policies and authentication measures across the environment is imperative in minimizing operational complexities and maximizing security. This solution provides policy enforcement and access control methods in a unified approach across all layers of the solution in order to address both complexity and security concerns.

Visibility

Data centers are becoming pliable in scaling to accommodate new virtual machines (VMs) and services. Server virtualization technologies, such as vMotion, enable servers to be deployed in and moved between multiple physical locations with minimal manual intervention. As VMs move and traffic patterns change, security administrators face challenges when attempting to actively monitor threats in the infrastructure. This architecture leverages threat detection and mitigation capabilities with state-of-the-art IPS appliances and cyber-threat-detection applications. This architect dynamically analyzes and correlates alarm, data, and event information to identify threats, visualize the attack paths, and also provide possible enforcement response options.

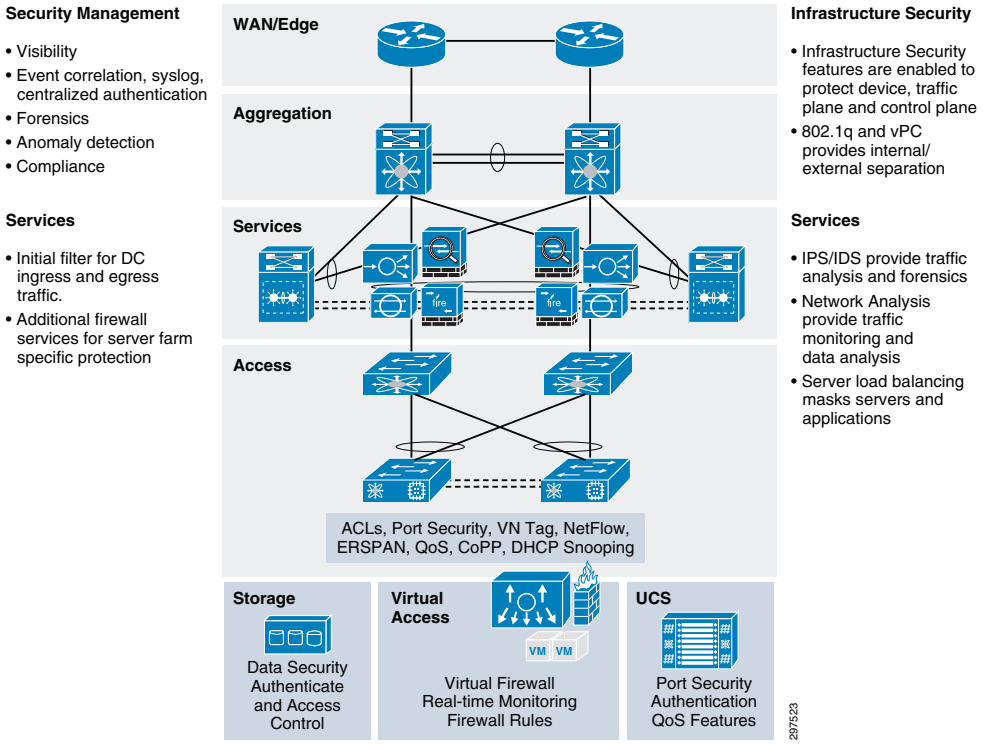
Resiliency

Resiliency implies that endpoints, infrastructure, and applications in multi-tenant environments are protected and can withstand attacks that would otherwise cause service disruptions, data exposure and unauthorized access. Proper infrastructure hardening, application redundancy, and firewalls are some of the approaches needed to achieve the desired resiliency.

VMDC Cloud Security Control Framework

Figure 2-2 shows a high level overview of the VMDC Cloud Security solution framework.

Figure 2-2 VMDC Cloud Security Solution Framework



The framework addresses three categories of security:

- Infrastructure Security, page 2-3
- Security Services, page 2-4
- Management Security, page 2-4

Infrastructure Security

Infrastructure security features protect devices and the network traffic and control planes. Key infrastructure security elements include:

- Internal and external separation using 802.1q and virtual port channels (vPCs)
- Storage separation, redundancy, and security (data-at-rest encryption)
- Industry standards and regulatory compliance, focusing on Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS)
- High availability (HA) and redundancy

Security Services

To provide end-to-end security in a multi-tenant cloud deployments, service providers need to deploy various security services. These security services, or features, can be offered to all the tenants or based on the service level. For example, for card processing customers, service providers must be providing firewall, and encryption services. Similarly, any high availability application requires load balancing services. The following security services are implemented in Cloud Security 1.0.

- Intrusion prevention systems (IPS) and intrusion detection systems (IDS) provide traffic analysis and forensics
- Network analysis provides traffic monitoring and data analysis
- Server load balancing masks servers and applications
- Line-rate NetFlow using Cisco NetFlow Generation Appliance (NGA)
- Intelligent centralized log monitoring using Splunk
- Centralized threat monitoring and detailed forensics using Cisco Cyber Threat Defense (CTD)
- Perimeter firewall services
- Remote Access VPN (RA-VPN) services
- Additional compute firewall services for server farm protection using VSG (virtual security gateway)

Management Security

When deploying a multi-tenant cloud data center, service providers need to protect their assets and tenants from security breaches. In a multi-tenant environment, there may be multiple admins managing the infrastructure, applications, and security, and there may be tenant admins accessing their virtual data center. To protect these activities, service providers need to conscientiously address the following:

- Visibility using Cisco CTD
- Event correlation and syslog using Splunk
- Centralized authentication using Cisco Secure Access Control Server (ACS)
- Segmented management traffic and data traffic, with additional firewall services between management plane and data plane

Secure Data Centers for Public and Private Cloud Providers

Aspects of security for secure cloud data centers include:

- Compliance, page 2-7

Physical Data Center Security

This includes having secure physical locations and controlled physical access to buildings and data center and network devices. Data centers must have badged or biometrically controlled access for data center administrators and maintenance personnel only. Physical data center security also applies to power management and heating/cooling equipment.

Note Physical data center security outside the scope of this guide.

Network Infrastructure Security

To secure the network infrastructure, SPs must protect and secure the physical and virtual infrastructure. For VMDC Cloud Security 1.0, the infrastructure is made up of the following elements:

- Data center border routers
- Data center edge/aggregation switches
- Access switches
- Load balancers
- Firewalls
- FirePOWER Next Generation Intrusion Prevention System (NGIPS)
- Compute, including Fabric Interconnect and Cisco Unified Computing System (UCS) chassis
- Storage area network (SAN) storage
- Cisco Nexus 1000V virtual switch
- Management components
- Cisco Virtual Security Gateway (VSG)

To provide network security, each element must be deployed redundantly so that the data center can sustain an element failure in any layer. For example, failure of an edge switch, load balancer, or IPS should not result in a system failure. We also recommend multiple paths among the infrastructure elements to protect data center integrity in case of a link failure in any layer.

Content Security

The Cisco Hosted Security Solution (HSS) validated design includes email and web security virtual appliances, ESAv and WSAv, to provide content security services. The HSS solution will reside in the service provider data center, and can be managed directly by the service provider, Cisco Smart Ops team, or a third party managed service provider.

For further details, refer to the HSS Design Guide.

Data Security

To protect a cloud data center in which multiple tenants use the same infrastructure, data paths must be secured so that intrusions and malware are detected and blocked. At a minimum, data must be secured using encryption, both while data is in transit and data at rest.

The data path can be north-south (server to client) and east-west (between VMs). For example, consider a tenant in which departments must be separated so that the departments cannot access applications in other departments. This can be achieved using multiple security elements, such as physical firewalls, NGIPS, and VSG that provide access control in the virtual environment.

Operating System Security and Hardening

We recommend updating the network infrastructure, virtual and physical systems, and applications to the most recent validated releases to ensure that no known security vulnerabilities are present. Install antivirus software and all operating patches and keep them current.

Secure Access Control

In multi-tenant data centers, cloud administrator can potentially access the entire infrastructure, and may have remote access, along with local access, to manage it. Because the infrastructure is the heart of the data center, all communication among devices in the data center must be encrypted; no unencrypted connections to any device should be allowed. For example, accessing a device over a Web interface must use HTTPS using Secure Socket Layer (SSL) 2.0 and higher). HTTP must not be enabled for web portal access.

To reduce security risks when accessing the data center, we recommend implementing RBAC to control access so that administrators have access only to systems for which they have administrative responsibilities.

For example, cloud administrators are typically responsible for the data center infrastructure and may not need access to the individual tenants and applications. Similarly, database and other services and application administrators should not have access to the data center virtual and physical infrastructure, but need access to certain portals. If an SP gives access to a tenant administrator to perform tasks in the SP virtual environment, the access must be read only or otherwise restricted to reduce security breach risks.

Network Visibility and Operation Intelligence and Monitoring

In environments for SPs and large enterprises having SP-type deployments, in which multiple tenants access the same physical and virtual data center infrastructure for services, complete network visibility is required. Centralized logging and event monitoring potentially helps in operations and maintenance. CTD and the third-party logging and monitoring appliance Splunk can provide the required visibility.

Centralized logging, monitoring large amounts of data, and recording transaction history is required for regulatory compliance for FISMA, HIPAA, and PCI DSS.

Compliance

When deploying public cloud data centers, SPs and large enterprises must comply with various industry standards and regulatory requirements, such as FISMA, HIPAA, and PCI DSS. The compliance requirements are based on the provided services.

For financial institutions and onboarding a financial institution or any type of card payments, data centers must comply with PCI DSS. Similarly, for health-care enterprises, data centers must comply with HIPAA standards to secure patients records and other medical research and communications. Data centers used by federal and defense agencies or contractors must comply with FISMA standards to ensure that communications and records are secure and that any compromise results in minimal and isolated breaches.

Solution Components

Table 2-1 summarizes the major solution components.

Table 2-1 VMDC Cloud Security 1.0 Solution Components

Components	Hardware
WAN EDGE	ASR 1000
DC AGGREGATION	Nexus 7000
FIREWALL	ASA 5585
IPS	FirePower IPS 8250
FIRESIGHT MANAGEMENT CENTER	DC 1500
NETFLOW GENERATOR	NGA 3240
LOAD BALANCER	CITRIX SDX 20550
DC ACCESS	Nexus 5548
UCS	UCS 5108 chassis, B200 M3, 2208 IOM
VIRTUAL SWITCH	Nexus 1KV
CISCO THREAT DEFENSE	Collector
LOG MONITORING	Splunk
STORAGE	NETAPP FAS 6080/6040
Virtual Firewall	VSG
Hypervisor	VMWare vSphere 5.1
Virtual Network Management Center	PNSC

CHAPTER 3

Cloud Security Design Details

Data security breaches, intrusions, and malware attacks occur many times every day and can be active for long periods without system owners even detect the breaches. Often, detection occurs after the damage is done, and can require huge efforts to mitigate. Successful attacks can hurt reputations, cost lots of money, and erode customer trust.

Most of the time malware takes at least a week or two to detect and identify. Due to this length of duration it is extremely difficult and sometimes impossible to identify infected devices on the network. It is critical to identify malware infection as quickly as possible so that appropriate action can be taken to quarantine an infection, stop it from spreading, and clean infected systems.

When SPs and enterprises deploy cloud data centers, they must determine security requirements based on the type of deployment and the services being provided. Different vertical industries require different levels of data center and network security when deployed in the cloud.

To address these issues, the VMDC Cloud Security 1.0 solution focuses on guidance and gap analysis to mitigate cyber threats and security risks and enable cloud providers to achieve industry standard compliances efficiently and cost effectively reducing huge operation cost.

To deploy this architecture and support various vertical industries such as, health care, finance, and federal government, the VMDC Cloud Security 1.0 solution integrates additional critical security components with the VMDC 2.3 reference architecture to provide better, more efficient security and compliance.

When cloud services are provided in multi-tenant environments in which multiple tenants share the same network infrastructure and compute and storage resources, the separation, segmentation, and security of each tenant is extremely important.

Secure separation, or multi-tenancy, separates workloads and virtual machines (VMs) to meet tenant (customer) separation, security, compliance, and service-level agreement (SLA) requirements while sharing a compute, 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 share the same physical servers and networks.

Data centers based on Virtualized Multiservice Data Center (VMDC) reference architecture consist of network, storage, and compute resources. Such data centers are typically interconnected and provide access to WANs, IP and Next Generation Networks (NGN), and the public Internet. VMDC-based data centers support multi-tenancy and multi-services, and provide management elements for administrative functions, orchestration (cloud portals, service catalog, and workflow automation), and assurance.

VMDC 2.3 Reference Architecture

The VMDC 2.3 reference architecture is a hierarchical layered model based on virtual port channel (vPC) technology. The benefits a hierarchical model provides, include scalability, resilience, performance, maintainability, and manageability. The hierarchical design represents a structured approach to building data center infrastructures, enabling relatively easy expansion in modular increments.

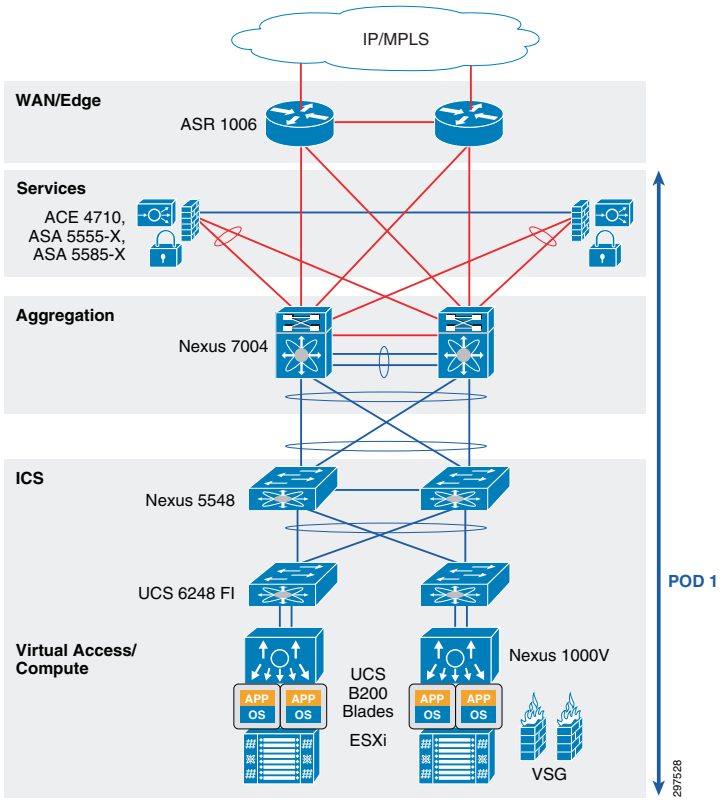
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-3/design_guide/VMDC_2-3_DG.pdf

Redundant nodes and links at each layer ensure no single points of failure, while link aggregation can be engineered for optimal bandwidth and performance. Devices in each layer perform similar functions, and this consistency simplifies troubleshooting and configuration. This results in easier, less expensive maintenance and plays key roles in security and compliance.

In data center deployments, WAN/provider edge (PE) routers act as a perimeter to the enterprise WAN or service provider (SP) IP/NGN backbone and the public Internet. These perimeter nodes may be dedicated to Layer 3 (L3) routing functions or may provide multiple services, such as Layer 2 (L2) interconnects between data centers along with L3 services.

Figure 3-1 shows the physical topology of the VMDC 2.3 reference architecture.

Figure 3-1 VMDC 2.3 Reference Architecture Physical Topology



In the VMDC 2.3 reference architecture, the infrastructure comprises of Cisco Nexus 7000 Series switches serving as aggregation nodes, and Cisco Nexus 5000 Series switches serving as access nodes. These switches support fine-tuning of port capacity and bandwidth to the level of aggregation or access density required to accommodate current and anticipated scale requirements. VMDC 2.3 was validated with ACE 4710 load balancer at that time, and now it is recommended to use Citrix SDX.

In the VMDC Cloud Security 1.0 reference architecture, Cisco ASR 1000 Series Aggregation Services Routers (ASR 1000) are used as WAN/PE routers, Nexus 7004 switches are used as aggregation devices, and Nexus 5548 switches are used as access devices. As shown in Figure 3-1, in the services layer the Cisco Adaptive Security Appliance (ASA) 5585 is used as a physical appliance for firewall protection.

Figure 3-2 shows the logical topology of the VMDC 2.3 system.

Figure 3-2 VMDC 2.3 Reference Architecture Logical Topology

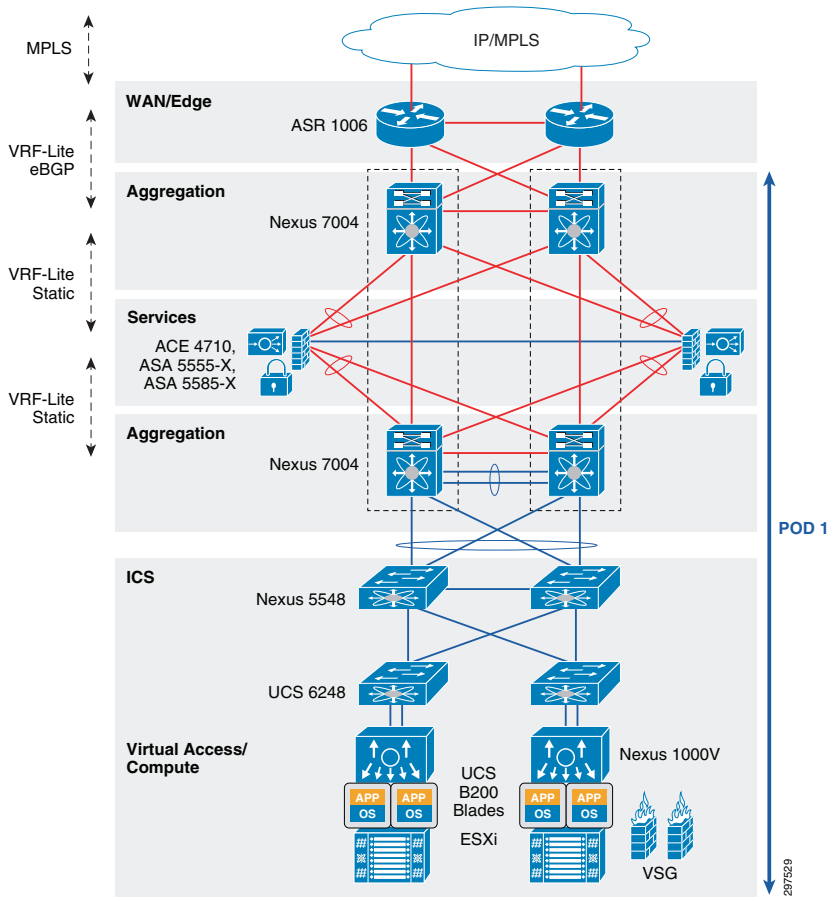
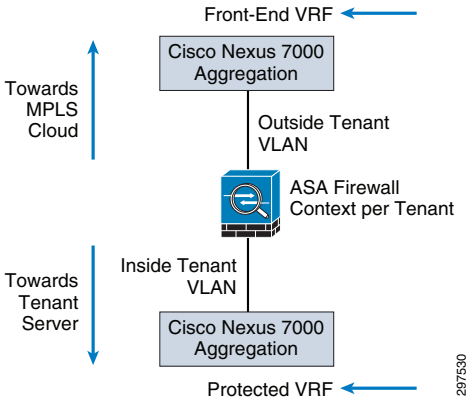


Figure 3-3shows how the Nexus 7004 aggregation switches are logically split to support front-end virtual routing and forwarding (VRF) and backend-protected VRF.

Figure 3-3 Nexus 7004 Aggregation Switches Supporting Front-End and Back-End VRF



In the VMDC 2.3 reference architecture, ASA firewalls are deployed in multi-context L3 routed mode. Static routes are defined on the Nexus 7004 switch that direct traffic for each tenant to a specific outside VLAN toward the ASA. After the ASA receives traffic on a tenant context, the ASA applies the necessary security policies and maps the traffic on the inside tenant VLAN. The Nexus 7004 switch receives this on a separate inside VRF (protected VRF) and then maps the L3 traffic to a tenant L2 VLAN toward the compute stack.

VMDC Cloud Security Reference Architecture

The VMDC Cloud Security 1.0 reference architecture is based on the VMDC 2.3 vPC-based reference architecture. The layers and components are similar to VMDC 2.3, with the addition of security elements (Figure 3-4).

Figure 3-4 VMDC Cloud Security 1.0 Security Elements

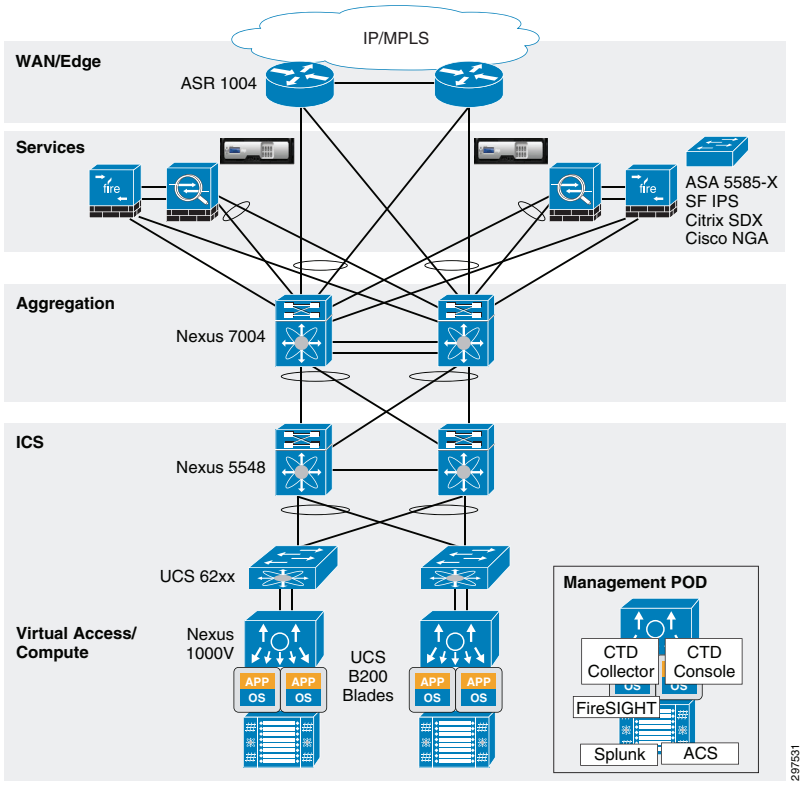
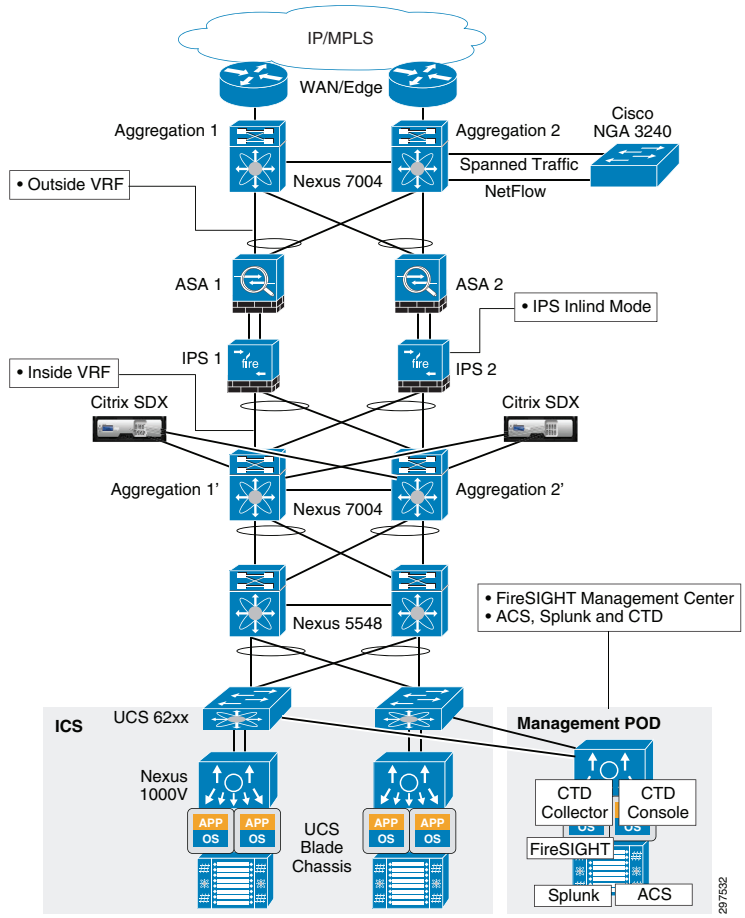


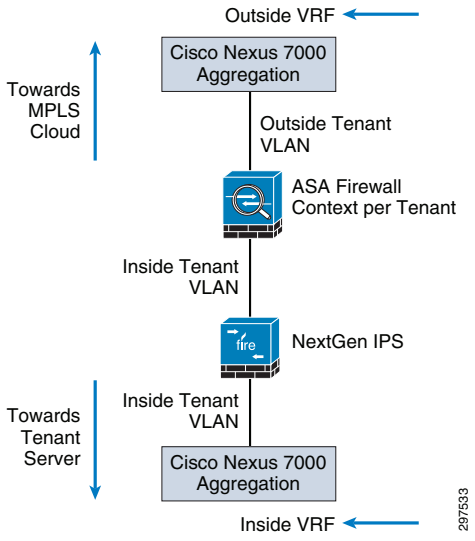
Figure 3-6 shows the VMDC Cloud Security 1.0 logical topology

Figure 3-5 VMDC Cloud Security 1.0 Security Logical Topology



As shown in Figure 3-6, tenant traffic that goes to the ASA firewall goes through NGIPS because NGIPS sits in line, with physical connectivity between the ASA firewalls and Nexus 7004 aggregation switches.

Figure 3-6 Traffic Flow—Nexus 7004 Switches, ASA, and NGIPS



NGIPS, deployed in transparent bridge mode, inspects traffic based on VLAN tags per tenant. When traffic reaches the inline NGIPS, NGIPS inspects traffic based on the tenant VLAN configuration and applies access policies and other deep inspection policies.

VMDC Cloud Security 1.0 Tenant Containers

The VMDC 2.3 reference architecture supports multiple network containers, which are also called consumer models. The consumer models are described in greater detail in VMDC 2.3 documentation.

This section describes the consumer models validated for VMDC Cloud Security 1.0. VMDC Cloud Security 1.0 supports the previously defined VMDC 2.3 consumer models, the same concepts of security features can be applied to other VMDC architectures. However, VMDC Cloud Security 1.0 validation focuses on Gold and Copper containers, which cover most VMDC 2.3 public and private cloud deployments.

Depending on VMDC container type, traffic may or may not go through security devices, based on subscribed services. However, because SPs must protect their data centers, traffic entering and leaving a multiservice data center must be monitored and inspected, and complete data center visibility is required. Hence, the VMDC 2.3 Gold and Copper network containers (which contain the ASA based perimeter FW service) are relevant for inserting NGIPS services as part of this VMDC Cloud Security 1.0 solution validation. It is also to be noted that while the security concepts in this solution are overlaid on the VMDC 2.3 architecture and container models, the same concepts can also be applied to other VMDC architectures like VMDC 3.0 etc.

To monitor all traffic, even traffic that does not go through a firewall and other security devices, we recommend using NetFlow to capture traffic from various locations in the data center, and using Syslog from all key network and security elements, including but not limited to aggregation, access, and virtual switches, along with firewalls, to provide complete data center visibility.

VMDC Cloud Security 1.0 Gold Container

A Gold container, with perimeter firewall, VSG, NGIPS, and server load balancer services, provides a higher degree of security and availability because each gold tenant is assigned a separate context or virtual firewall instance. Traffic for this container goes through NGIPS inspection, providing a higher degree of security for the tenant.

As shown in Figure 3-7, an NGIPS is physically in line between the ASA firewall and the Nexus 7004 switch. The traffic for the gold tenant received on the tenant outside VRF is first sent through the ASA firewall context, which applies the necessary access control policies and sends out the traffic on the gold tenant VLAN. Traffic on the inside VLAN goes through NGIPS, which applies the necessary inspection policies and passes the traffic to the Nexus 7004 aggregation switch, into the gold tenant inside (protected) VRF.

Figure 3-7 VMDC Cloud Security 1.0 Gold Container Topology

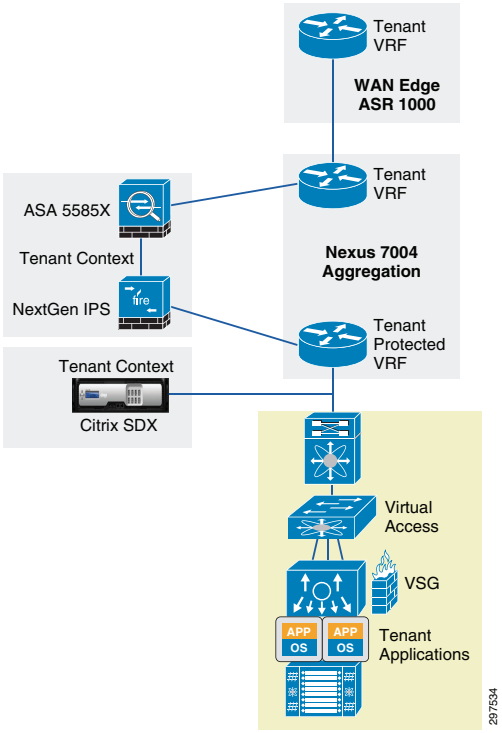
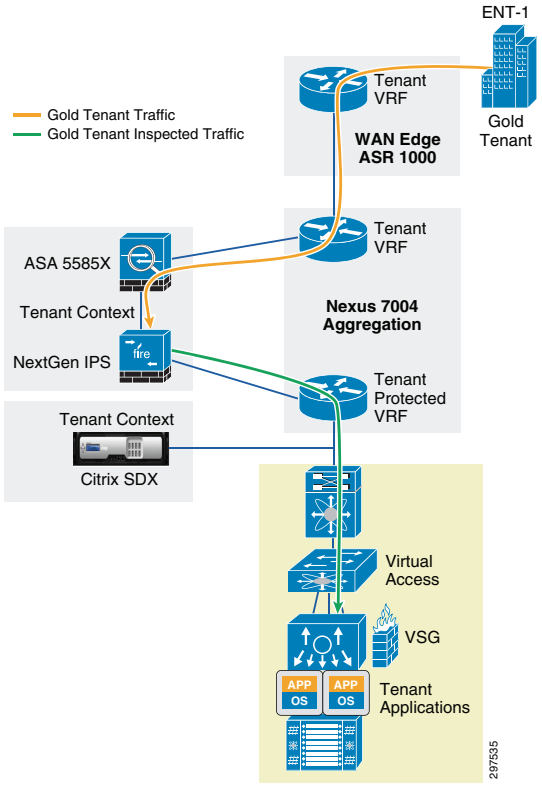


Figure 3-8 shows the Gold tenant traffic flow in VMDC Cloud Security 1.0.

Figure 3-8 VMDC Cloud Security 1.0 Gold Tenant Traffic Flow



VMDC Cloud Security 1.0 Copper Container

This tenancy model, designed to provide higher tenancy scale in VMDC 2.3 deployments, is suitable for Internet access to cloud resources. The Copper container is useful for SMB customers that require one VLAN and a handful of VMs in the cloud. Such customers require isolation and security, but typically do not want to pay higher fees for using their own virtual firewall context or deep packet inspection (DPI). The Copper container is designed such that all Copper tenants share the same VFW context. Copper containers consume fewer firewall contexts and VRF/BGP resources on the WAN edge and Nexus 7004 nodes.

The Copper tenant service level is generally lower than the Gold tenant service level. SPs may not want to use NGIPS resources to inspect copper tenant traffic, which may not require the higher level of security.

In a VMDC Cloud Security 1.0 Copper container, tenant traffic shares the global VRF when entering the data center. This saves some resources because there are fewer VRFs on the Nexus 7004 aggregation switch. Multiple Copper tenants also share a firewall context. The firewall applies the necessary access control policies and passes Copper tenant traffic back to the aggregation switch. Because NGIPS physically sits in line between the firewall and the aggregation switch, Copper tenant traffic (each Copper tenant has their own VLANs) is marked as trusted; NGIPS does not inspect Copper tenant traffic.

Figure 3-9 shows the VMDC Cloud Security 1.0 Copper container topology.

Figure 3-9 VMDC Cloud Security 1.0 Copper Container Topology

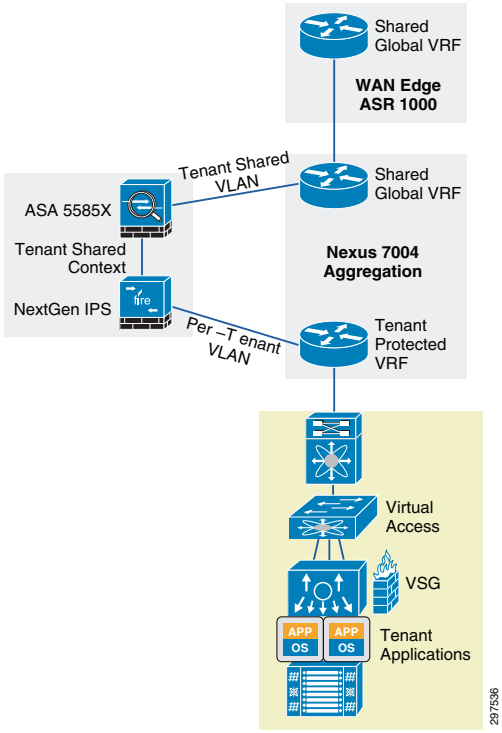
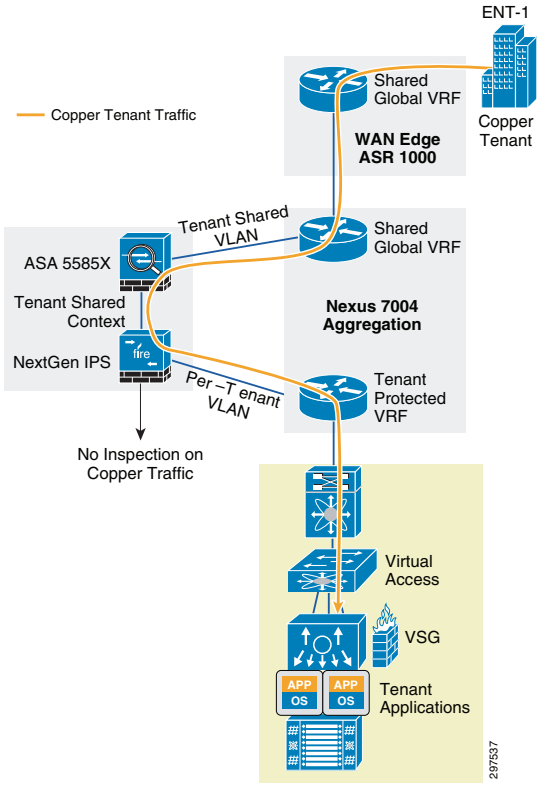


Figure 3-10 shows the Copper tenant traffic flow in VMDC Cloud Security 1.0.

Figure 3-10 VMDC Cloud Security 1.0 Copper Tenant Traffic Flow



VMDC Cloud Security 1.0 Bronze Container

Tenants boarded on Bronze containers maintaining their own separation to keep the threat localized in one container. On the other hand Bronze tenants receive the virtual firewall services VSG to provide intra tenant separation and security.

The Bronze container is the simplest and the most basic container; its traffic does not go through a firewall or NGIPS, even though the firewall and NGIPS are connected inline to the aggregation node.

Figure 3-11 shows the VMDC Cloud Security 1.0 Bronze container topology.

Figure 3-11 VMDC Cloud Security 1.0 Bronze Container Topology

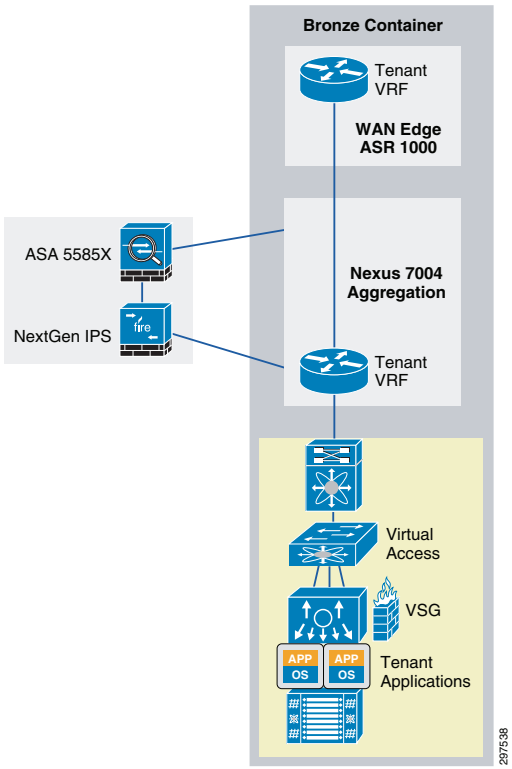
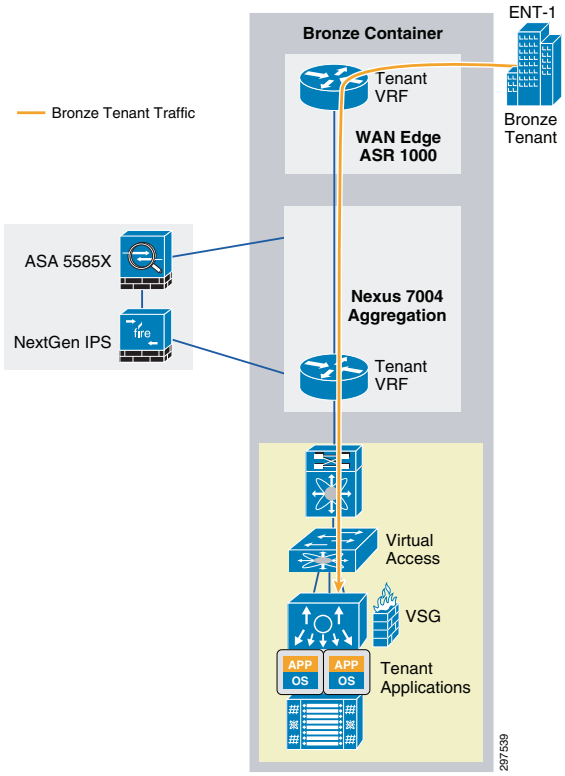


Figure 3-12 shows the Bronze tenant traffic flow in VMDC Cloud Security 1.0.

Figure 3-12 VMDC Cloud Security 1.0 Bronze Tenant Traffic Flow



VMDC Cloud Security 1.0 Silver Container

Tenants boarded on Silver containers do not receive security services except for VSG from the cloud.

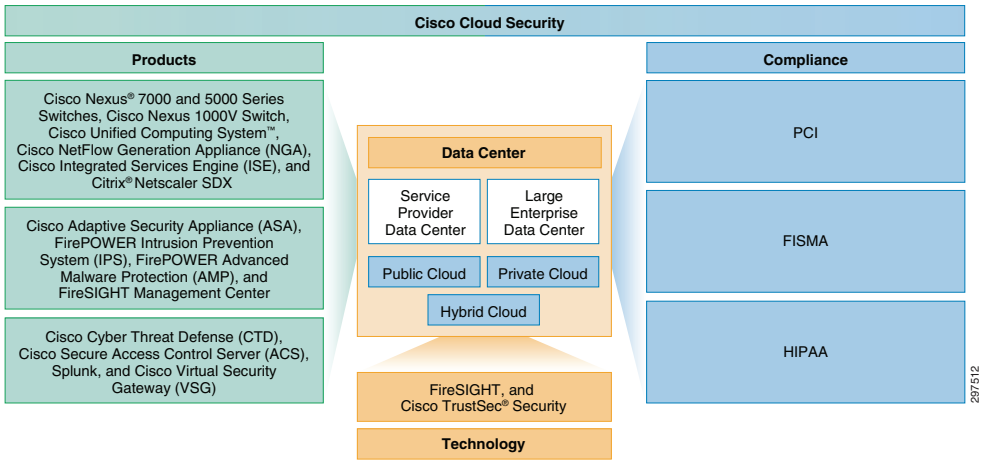
The Silver container is just like the bronze one with optional one-arm load balancer capability. The Silver container traffic does not go through a firewall or NGIPS, even though the firewall and NGIPS are connected inline to the aggregation node. For further details, refer to the VMDC 2.3 design guide.

Note The Silver Container model is not tested in VMDC Cloud Security release 1.0.

VMDC Cloud Security Solution Fundamental Pillars

The Virtualized Multiservice Data Center (VMDC) Cloud Security solution is built on three fundamental pillars. Figure 3-13 shows a holistic view of the VMDC Cloud Security 1.0 solution and its fundamental pillars: Products, Technology, and Compliance. These in turn enable service providers (SPs) to securely deploy public, private, and hybrid cloud data centers based on the multi-tenant VMDC 2.3 architecture.

Figure 3-13 Fundamental VMDC Cloud Security 1.0 Pillars



Key functionality covered in this solution includes:

- Tracking suspicious activity and threats
- Re-mediating vulnerabilities and mitigating attacks
- Network behavior analysis
- Active traffic monitoring in all directions
- Dedicated flow analysis for threat detection, behavioral analysis and forensics
- Centralized log collection from network and storage devices
- Industry standards and regulatory compliance

An effective security design requires complementary security services at appropriate points in the data center network, including:

- Defending the data center from unauthorized users and outside attacks
- Preventing intrusion and malware
- Defending the tenant edge with a proven firewall to secure the virtual and cloud infrastructures
- Assigning virtual machines (VMs) to segmented trust zones in the network and enforcing access policies at the virtual server level
- Providing centralized multi-tenant policy management
- Supporting VM mobility
- Separating security, network and server administrator duties
- Secure data center and applications access
- Scalability with the rest of the cloud infrastructure

VMDC Cloud Security 1.0 is based on the VMDC 2.3 virtual port channel (vPC)-based reference architecture. To provide more effective and robust security, VMDC Cloud Security 1.0 adds the following security elements:

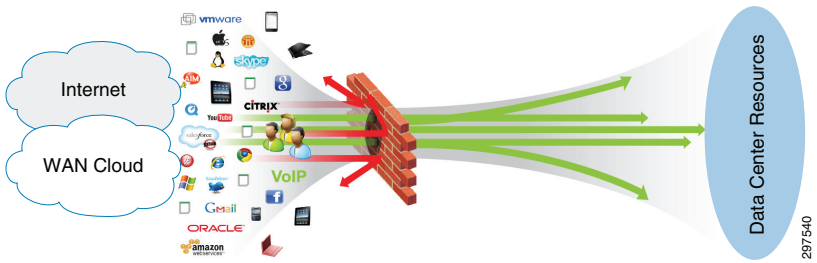
VMDC Cloud Security Design Considerations

The following Cloud security design considerations are recommended:

Access Control

In the VMDC Cloud Security 1.0 reference architecture, a pair of ASA 5585 access control firewalls is used to minimize the impact of unwanted network access to the data center. Figure 3-14 illustrates this access control.

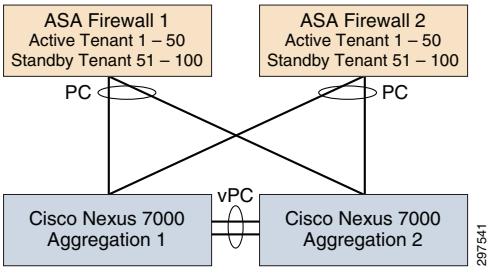
Figure 3-14 Access Control Using the ASA 5585 Firewall



The ASA 5585 firewall pair is used in active/active mode and is configured in multi-context routing mode. The secure inside network must be in a separate subnet from client subnets and the outside network. In multi-context mode, virtual contexts are configured on the ASA firewall pair, dividing each into multiple logical firewalls. Each logical firewall can support different interfaces and policies.

On each of the ASA 5585 firewall pair, half of the tenant contexts are active and half of the tenant contexts are inactive. This protects all tenants; in the event that one of the ASA 5585 firewall pair fails, the remaining firewall successfully supports all tenants, as shown in Figure 3-15.

Figure 3-15 ASA 5585 Pair in Active/Active Mode



The ASA 5585 firewall pair create the dual-home to the data center aggregation nodes using two 10-Gigabit Ethernet (10 GbE) links for resiliency. The two links on each firewall are configured as an EtherChannel to provide both load balancing and responsive failure recovery. The vPC feature on the Cisco Nexus 7000 data center aggregation switches enables the firewall EtherChannel to span the two data center aggregation switches while appearing to be connected to one upstream switch. This EtherChannel link is configured as a VLAN Trunk to support access to multiple secure VLANS in the data center.

Site to Site VPN

In VMDC Cloud Security 1.0, data center ASA may be used for site-to-site VPN which potentially eliminates the need for another physical VPN concentrator. For further details, refer to the link below:

http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/112153-ccp-vpn-asa-router-config-00.html

Secure Remote Access VPN

A pair of ASA in active/standby is required to provide secure remote access VPN (RA-VPN) services from the service provider cloud. For further details, refer to the link below:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-3/design_guide/VMDC_2-3_DG.pdf

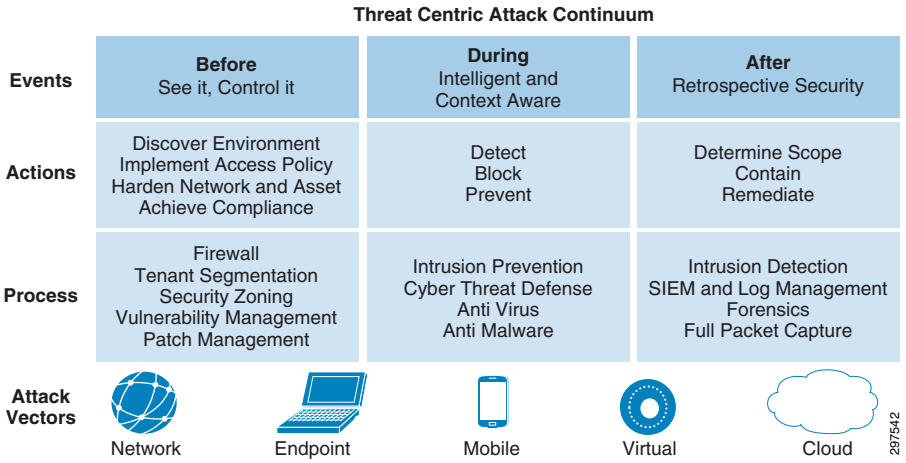
NGIPS Integration

In VMDC Cloud Security 1.0, FirePOWER Next Generation Intrusion Prevention System (NGIPS) performs line-rate deep traffic inspection.

To secure data center deployments, SPs require complete visibility into their entire networks, for users, infrastructure, devices, services, and resources. To prevent all threats, SPs must cover the full attack continuum that occurs before, during, and after attacks. Following these steps prevents the occurrence of the same threat.

Figure 3-16 shows the steps and elements help achieve strong, effective defense against the threat-centric attack continuum.

Figure 3-16 Threat-Centric Attack Continuum



As shown in the above diagram, with all the mobility and virtualization, there are now many different attack vectors such as Mobile users, Virtual desktops etc. This increases the chances of threat and security concerns.

In VMDC Cloud Security Release 1.0, the ASA firewall is used for access control. This protects the data center from outsiders and limits the access based on the policies defined for trusted users and applications. This allows only trusted users/tenants into the data center, but if the trusted users send malicious traffic, the firewall cannot detect it.

To protect the data center during the normal operation, line rate non-blocking inspection is a necessity. The Cisco FirePOWER next generation IPS provides the capability to inspect all the traffic in and out of the cloud data center at a line rate. The next generation IPS provides malware protection and intrusion prevention by stopping the exploits, hackers, attacks. It also provides application control and URL filtering which can be implemented on a per tenant basis. During the normal operation, Cisco Cyber threat defense provides in-depth visibility by collecting Netflow and NSEL streams of data. This can help cloud providers to actively monitor any threat.

In case of data security breach, cloud providers need tools that isolate the incident without compromising the entire the data center. So that the tenant can trace the breach to its source, the provider can use multiple security techniques, such as, proper separation of tenants, Intrusion detection, and log monitoring. The log monitoring also helps later in terms of investigation and forensic activity.

Integrating FirePOWER NGIPS into the VMDC Cloud Security 1.0 reference architecture provides point-in-time detection of any malware or threat, leveraging big data analytics and a continuous analysis capability to confirm an infection, trace its path, analyze its behavior, re-mediate its target, and report its impact regardless of when a file is determined to be malware.

NGIPS enables SPs to look deeply into a device and provides the following information:

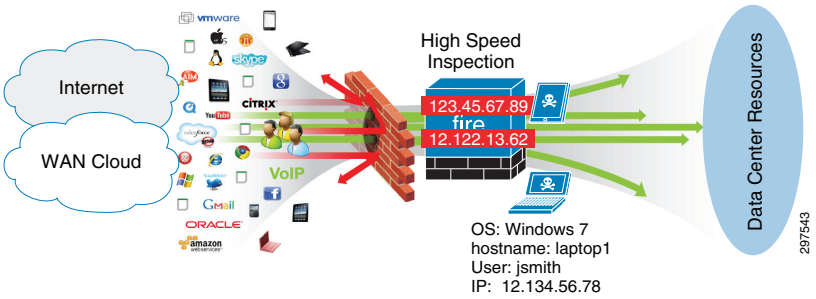
1. How did the threat get onto the device?
2. How serious is the threat?
3. What communications were made from the infected device?
4. What is the chain of events?

This information enables SPs to take timely, appropriate action to avoid downtime and provide the most secure environment to their tenants.

Policy and control using firewalls and other techniques reduce only the surface area of an attack. In theory this approach makes sense, but in practice this approach fails when trusted persons or devices initiate attacks. No matter how large or small a security gap is, the bad people will find it and try to exploit it. It is no longer safe to assume that what is permitted in a network or data center is good. Having a high speed inspection engine that can inspect all content traveling in and out of a data center to detect, understand and stop threats is the recommended way to ensure that identified threats can no longer enter the data center.

Figure 3-17 shows that even after deploying firewalls, infected traffic may get through it. Hence, high-speed inspection is required to block, mitigate, or quarantine such infections.

Figure 3-17 Threat Penetrations despite Firewalls and control policies



FirePOWER NGIPS combines the security of an industry-leading IPS with the power to control network access based on detected applications, users, and URLs.

In VMDC Cloud Security 1.0, NGIPS is deployed inline and can:

- Gather detailed information about hosts, operating systems, applications, users, files, networks, and vulnerabilities.
- Block or permit network traffic based on various network-based criteria, along with other criteria including applications, users, URLs, IP address reputations, and the results of intrusion or malware inspections.
- Be deployed in fail-safe or fail-open mode, depending on the deployment requirement.

Intrusion detection and prevention enables SPs to monitor data center network traffic for security violations and, in inline IPS deployments, enable them to block or alter malicious traffic. Intrusion prevention is integrated into access control, in which SPs can associate intrusion policies with specific access control rules. If network traffic meets the conditions in a rule, NGIPS can analyze matching traffic using an intrusion policy.

NGIPS can be deployed in fail closed or fail open modes. This feature enables service provider to decide what action need to be taken during the failure of an IPS appliance.

Table 3-1 shows the availability of the failure modes for the hardware models:

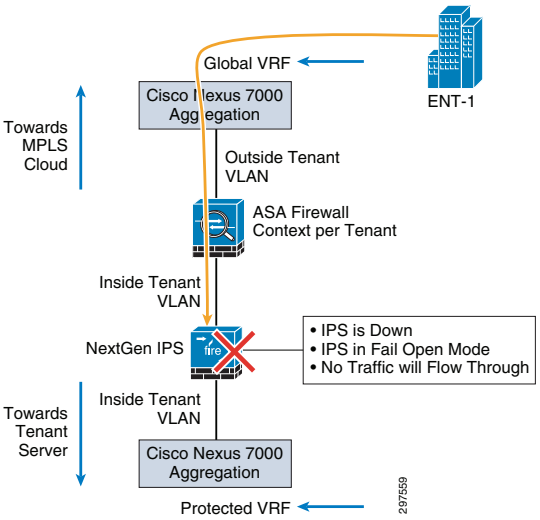
Table 3-1 Failure Mode Availability Based on Hardware and SFP Modules

IPS 8xxx Series with SFP Modules	IPS 7xxx Series with Fixed Port	IPS 7xxx Series with Fixed and SPF Module
Fail Close Only SFP Modules	Fail Open and Fail Close	Fail Open and Fail close on Fixed and Fail Close on SFP Module
Fail Open and fail Close SFP Modules		

NGIPS Fail Close Mode

As shown in Figure 3-18 fail close mode is supported on all NGIPS models. In fail close mode, NGIPS shuts down traffic through the appliance, so packets cannot pass through NGIPS sensor on any NGIPS interfaces.

Figure 3-18 Fail close Mode



The VMDC Cloud Security 1.0 solution supports fully redundant HA design for all links and network components. We recommend deploying NGIPS in a fail-safe mode so that a single appliance failure routes traffic to the secondary path and minimizes the downtime of any services running in the data center. When deploying NGIPS in a fail close mode, all inspection flows dropped from the failed NGIPS are picked up by the secondary NGIPS in the middle. The secondary NGIPS starts building the flows as more packets pass through.

Note To ensure no packet loss from inspection even if NGIPS picks up flows in the middle, or to deal with the asymmetrical traffic flows, the STRICT TCP enforcement box must not be checked at the IPS interface level during the initial configuration.

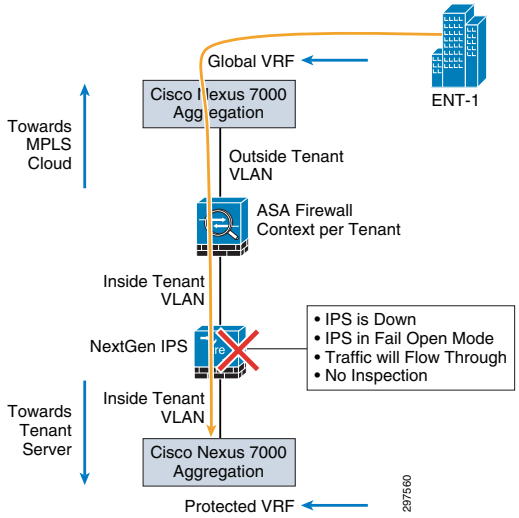
Note It is not recommended to deploy single NGIPS in a fail close mode. If a single NGIPS deployed in the data center inline between the aggregation and access layers, in case of NGIPS failure, all the services go down and no traffic or data can pass through the NGIPS appliance.

NGIPS Fail Open Mode

NGIPS fail open mode is available depending on hardware platform and interface module type used in the physical appliance. When NGIPS is configured in fail-open mode and there is a failure of either the appliance or ingress or egress links, the NGIPS appliance closes a mechanical relay in the appliance, enabling packets to flow through it. In this case, there is no data inspection or monitoring. Instead, traffic flows transparently without interruption of active services.

Figure 3-19 shows the flow of traffic during fail open mode.

Figure 3-19 Fail Open Mode Traffic Flow



When a failure occurs and NGIPS goes into fail open mode, some security gaps occur for the duration of the failure. During this time, any malware or intrusions that penetrate the data center using this route are not captured and impose a risk even after NGIPS recovers from the failure.

Note Recommendation is to configure redundant NGIPS in fail close (fail closed) mode. If a failure occurs on any side of a network or security component, this enables traffic to move to the second NGIPS.

SPs typically deploy VMDC in multi-tenant environments using overlapping IP addresses. This enables faster tenant deployment and minimizes operation costs for IP management and maintenance.

In VMDC deployments, overlapping IP address scheme for tenants prevents FireSIGHT Management Center and FireSIGHT technology from capturing and reporting based on unique IP addresses.

The following example shows an SP enabling the hosts monitoring feature on the FireSIGHT Management Center in an overlapping IP address environment:

1. Host A, with IP address 10.10.10.1, runs Linux in VMDC tenant container A; FireSIGHT Management Center detects a malware file.
2. Host B, with the same IP address (10.10.10.1) runs Windows in VMDC tenant container B; FireSIGHT Management Center detects an intrusion.
3. Host C, with the same IP address (10.10.10.1) runs a different version of Linux; FireSIGHT Management Center detects a malware file and receives the cloud disposition of unknown.

As noted, the three hosts have the same IP address although they belong to three different tenant containers. This creates a disordered database showing same host deployed with multiple operating systems, multiple versions of same operating system, a malware detection alert, an intrusion alert, and at the same time malware detect with unknown disposition.

In this situation, it is extremely difficult to locate the actual hosts and which tenant containers they belong to. In the preceding example, three hosts have issues in three tenant containers, and The SP may be unable to locate the exact host to take appropriate action to defend against the threats.

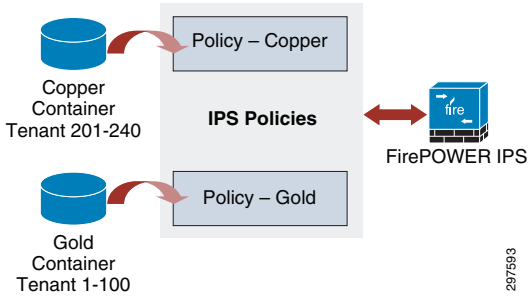
To overcome the overlapping IP address issue, we recommend using VLAN tagging to isolate hosts in each tenant container, as shown in the following example.

1. Host A, with IP address 10.10.10.1 and VLAN tag 100, runs Linux in VMDC tenant container A; FireSIGHT Management Center detects a malware file.
2. Host B, with the same IP address (10.10.10.1) with VLAN tag 200, runs Windows in VMDC tenant container B; FireSIGHT Management Center detects an intrusion.
3. Host C, with the same IP address (10.10.10.1) with VLAN tag 300, runs a different version of Linux; FireSIGHT Management Center detects a malware file and receives the cloud disposition of unknown.

Each host belongs to a specific VLAN in a tenant container, so for intrusion detection, FireSIGHT Management Center can notify the event using the VLAN tag. This enables SPs to pinpoint infected devices and take appropriate action to mitigate or quarantine them.

When deploying multiple tenants, each tenant will belong to a type of container, either Gold, Silver and so on, as shown below:

Figure 3-20 Multiple Tenant Container Types



Note When configuring an IPS policy per container type, all tenants on the container type receive the same policy. This helps service providers significantly in terms of operations and maintenance.

Note When performing changes to an IPS policy that impacts memory allocations (increase or decrease), the SNORT process may restart and the IPS sensor may not process packets for a short period of time. The period of time varies depending on the load and the number of polices applied. As a best practice, we recommend defining one policy per VMDC container model to improve performance. It is recommend that when modifying or adding new IPS polices policy changes should be carried out during scheduled maintenance windows. To inspect all the traffic during a maintenance window, we recommend diverting the traffic to the failover IPS within the data center before performing maintenance work to minimize any unforeseen downtime.

Use the Firesight Management Console to deploy intrusion policies with tiers of service. For example, you can define three IPS policies to represent three tiers of service:

- Gold Tier: Inline, blocking;
- Silver Tier: monitor only;
- Bronze Tier: limited or no monitoring

Any IPS policy can be referenced more than once in the Access Control policy, and events are separated by VLAN tags for different clients. This approach streamlines the IPS / IDS enforcement per rule in the Access Control policy. A rule in the Access Control policy can reference either a single client or entire tier of service.

For malware detection, FireSIGHT Management Center cannot use VLAN tag association; instead, SPs must build per-tenant file policies and assign the policies in malware rules to detect individual hosts in a tenant container. This enables SPs to isolate infected hosts in a specific tenant container for malware detection.

For application monitoring, we recommend enabling application discovery under the network discovery portion of FireSIGHT Management Center. In SP environments, tenant applications may use overlapping IP addresses. Although application discovery may have the same issues as hosts with overlapping IP addresses, this at least gives SPs a high-level view of what applications are running, and if there are any specific threats to these applications, FireSIGHT Management Center adjusts the threat level accordingly.

FirePOWER FireSIGHT Management Center

FirePOWER FireSIGHT Management Center provides a centralized management console and event database repository for FirePOWER NGIPS. FireSIGHT Management Center aggregates and correlates intrusion, file, malware, discovery, connection, and performance data, assessing the impact of events with indications of compromise. This enables SPs to monitor what data center devices report in relation to other devices, and to assess and control the activity that occurs in a data center.

FireSIGHT Management Center can be deployed in a fully redundant mode to ensure continuous operation. The FireSIGHT Management Center pair shares policies, user accounts, and configurations. Events are sent to both systems in the redundant pair.

FireSIGHT Management Centers periodically update each other on configuration changes, and changes made to one system are applied to the other. Each FireSIGHT Management Center has a five-minute synchronization cycle, but the cycles themselves can be out of synchronization by as much as five minutes, so changes appear within two five-minute cycles. During this ten-minute window, configurations may differ on the paired FireSIGHT Management Centers.

FireSIGHT Management Centers in a high availability pair share the following information:

- User account attributes
- Authentication configurations
- Custom user roles
- Authentication objects for user accounts and user awareness, as well as the users and groups that are available to user conditions in access control rules
- Custom dashboards
- Custom workflows and tables
- Device attributes, such as the device's host name, where events generated by the device are stored, and the group in which the device resides
- Intrusion policies and their associated rule states
- File policies
- Access control policies and their associated rules
- Local rules
- Custom intrusion rule classifications
- Variable values and user-defined variables
- Network discovery policies
- User-defined application protocol detectors and the applications they detect
- Activated custom fingerprints
- Host attributes
- Network discovery user feedback, including notes and host criticality; deletion of hosts, applications, and networks from the network map; and deactivation or modification of vulnerabilities
- Correlation policies and rules, compliance white lists, and traffic profiles
- Change reconciliation snapshots and report settings
- Intrusion rules, geo-location database (GeoDB), and vulnerability database (VDB) updates

When deploying HA FireSIGHT Management Centers, managed NGIPS are configured to send event data to both systems. If a system fails, SPs can use the redundant system to monitor the network without interruption.

When deploying redundant FireSIGHT Management Centers, both physical appliances must be identical, and both must run the same software and firmware versions. This protects the reporting and cloud disposition feature in case of single appliance failure without any downtime.

Table 3-2 compares the services available after a FireSIGHT Management Center failure when deploying one FireSIGHT Management Center with those available with a redundant FireSIGHT Management Center deployment.

Table 3-2 FireSIGHT Management Center Failure for Single and Redundant Deployments

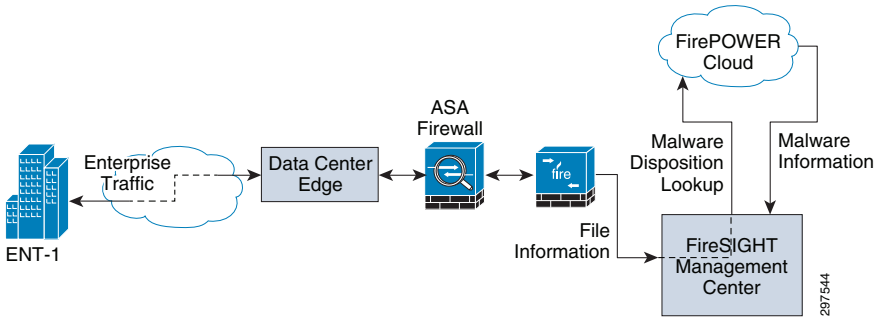
Services	Single FireSIGHT Management Center Appliance Failure	Redundant FireSIGHT Management Center Single Appliance Failure
FireSIGHT management center Monitoring & Reporting	No	Yes
URL Filtering	No	Yes
Cloud Disposition	No	Yes
Control Policy	Yes	Yes
New Configurations	No	Yes
IPS Event Collection on the Sensor	Yes	Yes
IPS Event Collection on the FireSIGHT management center	No	Yes
e-Streamer data from IPS Sensor to SEIM	Yes	Yes

Note FireSIGHT Management Center HA is outside the scope of VMDC Cloud Security 1.0.

FireSIGHT Management Center Cloud Connectivity

To establish the FirePOWER cloud connectivity the FireSIGHT management system need to have an IP connectivity to the cloud. To achieve the connectivity, the malware license installation has to be completed. Once the license is installed, configure the FireSIGHT management system with TCP port 32137 to establish the bi-directional cloud connectivity.

Figure 3-21 FireSIGHT Management Center Cloud Connectivity



Note In case of FireSIGHT management center failure (single FireSIGHT management center deployment model), the appliance will loose the capability of getting a malware disposition from the Cisco FirePOWER cloud.

Single FireSIGHT Management Center Deployment failure:

1. When using the single FireSIGHT Management Center deployment model, the network can no longer get malware and cloud dispositions from the FirePOWER cloud, and URL filtering no longer work.
2. The NGIPS appliance blocks malware based on a pre-configured malware policy.
3. Pre-configured control policies continue to work without FireSIGHT Management Center
4. The NGIPS appliance locally stores all events during the FireSIGHT Management Center failure. After FireSIGHT Management Center becomes available, NGIPS synchronizes events with Management system and updates all logs.

In FireSIGHT Management Center, the relationship between file type events and malware events is important. If a file policy is configured to perform malware cloud lookup, the returned dispositions can be one of the following:

- Clean
- Malware
- Unknown

When the disposition is clean, no action is taken and data flows normally. When the disposition is malware, FireSIGHT Management Center, based on its configuration, acts on the file and blocks it. If the disposition is unknown, the system keeps the file in a monitor mode to see whether the disposition changes to malware in the near future. If an unknown file type turns out to be malware, FireSIGHT Management Center blocks the file.

FireSIGHT Management Center System Requirements

Table 3-3 summarizes the system requirements for FireSIGHT Management Center.

Table 3-3 FireSIGHT Management Center System Requirements

	DC 750	DC 1500	DC 3500
System Memory	2 GB	6 GB	12 GB
Disk Storage for Event Data	100 GB	125 GB	400 GB
RAID Configuration	N/A	RAID 1	RAID 5
Max IDS Event Storage	20M	30M	150M
Max Flow Data Storage	50M	100M	500M
Max Sensors Registered	10	35	150
Max IDS Event Rate	2,000/sec	6,000/sec	10,000/sec
Max Flow rate	2,000/sec	6,000/sec	10,000/sec
Lights Out Management	Yes	Yes	Yes

Note The maximum number of NGIPS depends upon NGIPS type and event rate.

FirePOWER FireSIGHT is a discovery and awareness technology that collects information about hosts, operating systems, applications, users, files, networks, geo-location, and vulnerabilities to provide a comprehensive view of the data center network.

The FireSIGHT Management Center web interface provides a view of data collected by FireSIGHT. SPs can use this data to perform access control and modify intrusion rule states.

Access control is a policy-based feature that enables SPs to specify, inspect, and log traffic that can traverse their networks. An access control policy determines how the system handles network traffic. A policy that does not include access control rules handles traffic in one of the following ways (default action):

1. Block all traffic from entering your network.
2. Trust all traffic to enter your network without further inspection.
3. Allow all traffic to enter your network, and inspect the traffic with a network discovery policy only.
4. Allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies.

For VMDC Cloud Security Release 1.0, Copper and Gold tenants are validated. Copper tenants share the same firewall context and the Copper tenant traffic goes through the inline IPS. Because most Copper tenants are SMB customers who do not need additional security, this traffic does not require inspection. Marking traffic as Trusted, prevents inspection.

Note In this release, Bronze tenants were also tested, but this traffic does not go through the firewall and NGIPS

In VMDC Cloud Security 1.0, Copper tenants have separate server VLANs, even though they share the same firewall context and are segmented at L2. It is recommended to configure NGIPS with device fast-path rule in hardware for all the Copper or Silver tenants that may not require deep packet inspection.

SPs may include access control rules in access control policies to further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. A rule action is specified for each rule, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

In multi-tenant environments in which SPs use the overlapping IP addresses for tenants, the Cisco FirePOWER IPS can detect and mark per-tenant intrusion events based on VLAN tag. To get per-tenant malware events, SPs need to define per-tenant file policies.

Network-Based Advanced Malware Protection (AMP)

Network-based advanced malware protection (AMP) is a license based feature. AMP allows the system to inspect network traffic for malware in several types of files. Appliances can store detected files for further analysis. After NGIPS detects a file as a culprit, NGIPS submits the file to the FirePOWER cloud using FirePOWER FireSIGHT Management Center to perform a simple known-disposition lookup using the SHA-256 hash value of the file.

The following methods can determine whether a file is malware:

- **SHA-256 hash—**This method is fast and requires minimal communication with the FirePOWER cloud to get one of three malware dispositions for any file: Clear, Malware or Unknown. When malware lookup is based on file policy settings, NGIPS captures the file based on the tenant VLAN

tag and calculates the SHA-256 hash value. This value is sent to FireSIGHT Management Center, which forwards the value to the FirePOWER cloud for malware disposition. The cloud lookup time for the disposition is typically under 200 msec.

- **SPERO fingerprint**—When this is enabled, NGIPS collects static file attributes and transmits the SPERO signature to the FirePOWER cloud. This can identify malware even if the specific file SHA hash value has not been observed.
- **Sandbox file analysis**—This feature can extract files from the network flow and submit them to the FirePOWER cloud for evaluation. Submission can be configured to be automatic or manual.

  Automatic analysis is limited to Windows PE (executables) having unknown status. Manual submission supports a wide variety of file types, including MSEXE/DLL, JAR, PDF, SWF, DOC, DOCX, PPT, PPTX, XLX, XLSX, and RTF.

  Using this technique, files are executed in the sandbox environment. Execution results in a threat score; the file can be marked as malware based on its threat score. Getting a threat score can take from 5 to 10 minutes. Sandbox file analysis do not block files, but subsequent detection of these files based on the SHA-256 enables to do a block action on the file.

Depending on the security requirements and threat, service provider configured the system to submit files for dynamic analysis, which produces a threat score. Using this contextual information, service provider can configure the system to block or allow specific files. It is recommended to configure malware protection as part of the overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Table 3-4 shows different actions the FireSIGHT management center and IPS can take based on the file policy configurations.

Table 3-4 FireSIGHT Management File Lookup Behavior

File Policy Action	Default Behavior	Auto Dynamic File Analysis	SPERO Fingerprint	File Types
Detect Files	Log	No	No	All supported file types
Block Files	Block & Log	No	No	All supported file types
Malware Cloud Lookup	Log, SHA-256 Lookup	Optional (MS EXE)	Optional (MS EXE)	Malware File Types Only
Block Malware	Log, SHA-256 Lookup, block if malware	Optional (MS EXE)	Optional (MS EXE)	Malware File Types Only

Design Options for NGIPS in VMDC Cloud Security Architecture

The VMDC Cloud Security 1.0 architecture is based on the VMDC 2.3 vPC-based reference architecture to provide HA and better bandwidth between the vPC peers, such as between aggregation switches/access switches, and aggregation switches/services components.

In VMDC Cloud Security 1.0, NGIPS is deployed inline to enable SPs to protect entire data centers from attacks that might affect the availability, integrity, or confidentiality of hosts or devices in the SP network.

The VMDC Cloud Security 1.0 architecture is built so that traffic can flow asymmetrically when entering and exiting a data center. Because of asymmetrical data flows in data centers, NGIPS must be integrated into the architecture so that it is not affected by the asymmetrical traffic flow.

This section describes design considerations on how and where we can insert the FirePOWER next generation IPS in the VMDC 2.3 reference architecture in such a way that it will be less disruptive and provide scale and performance with high availability. There are multiple locations service provider may be able to insert the NGIPS within the VMDC 2.3 reference architecture. Below sections covered all such possibilities and provides the recommended method, that will integrate the NGIPS in such a way, the architecture integrity will not be compromised.

Inserting Multiple NGIPS at the Aggregation Layer (Recommended Design)

As shown in Figure 3-22, NGIPS can be inserted between the aggregation and access layer on each link to eliminate appliance failure as a single point of failure.

Figure 3-22 Inserting Multiple NGIPS between Aggregation and Access Layer

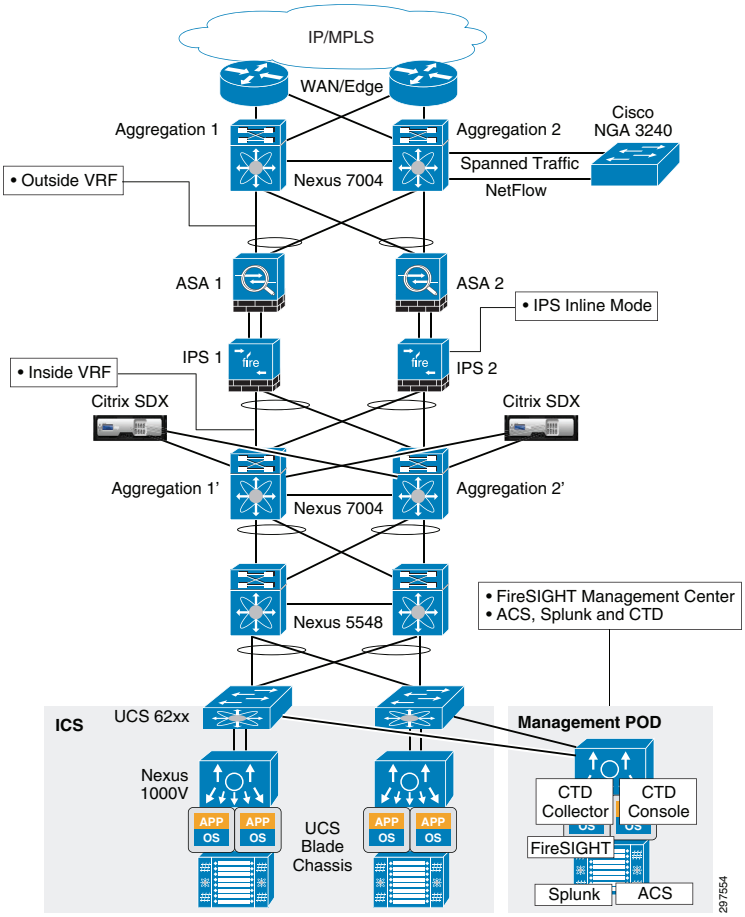


Table 3-5 summarizes the pros and cons of this deployment model.

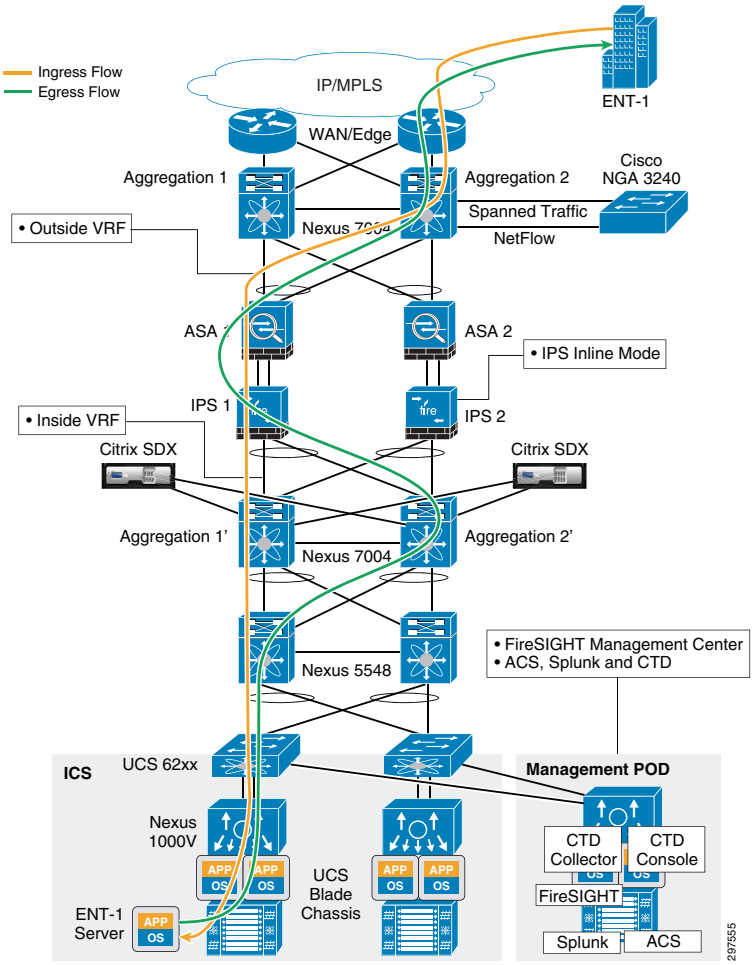
Table 3-5 Deployment Model Pros and Cons

Pros	Cons
Higher Scale than at the access layer	Some Issue with Asymmetrical traffic in case of one IPS failure
Protect north/south and some east west Traffic	
High Availability	
Easy integration within existing VMDC environment	

Note Require a pair of NGIPS per Compute Pod (Vblock or FlexPod) when deploying IPS at the access layer.

Figure 3-23 shows the data center ingress and egress traffic flows. Traffic may flow through one aggregation and access switch during ingress and may try to use the second access and aggregation switch on the egress path. Based on static routing configurations on the Nexus 7004 aggregation switches, traffic flows to specific ASAs from both aggregation switches as shown.

Figure 3-23 Ingress and Egress Traffic Flows



The VMDC Cloud Security 1.0 solution uses ASA in active/active mode. In this mode, each ASA services half of the data center tenants in an active state and rest of the data center tenants on standby. If an ASA fails, the second ASA can service all data service tenants without downtime.

To deploy NGIPS in a redundant mode, insert an NGIPS appliance physically inline between each Nexus 7000 aggregation switch and ASA firewall, as shown in Figure 3-24.

In this deployment model, traffic reroutes to the secondary path in the following situations:

1. Complete ASA firewall appliance failure
2. Complete NGIPS appliance failure
3. Both links fail between ASA and Nexus 7004 aggregation switch
4. One management link fails and one data link fails on ASA
5. Both links fail between ASA and NGIPS
6. Both links fail between NGIPS and Nexus 7004 aggregation switch

Figure 3-24 Traffic Flows with ASA Firewall and IPS Failure

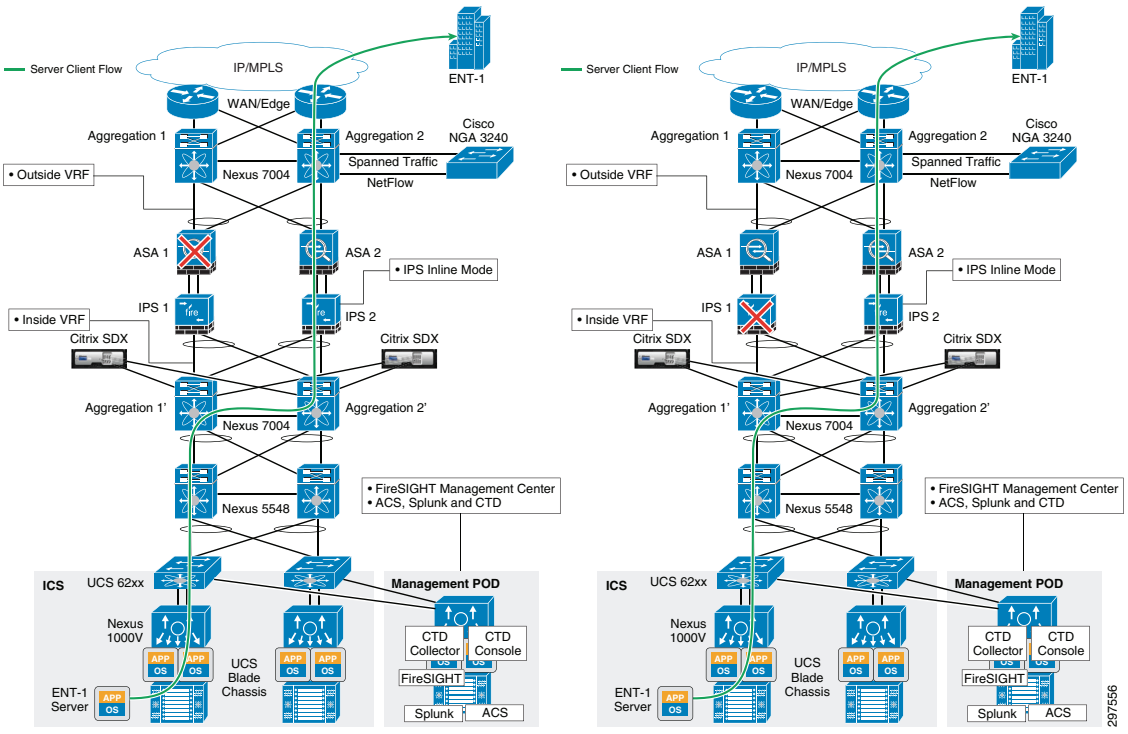
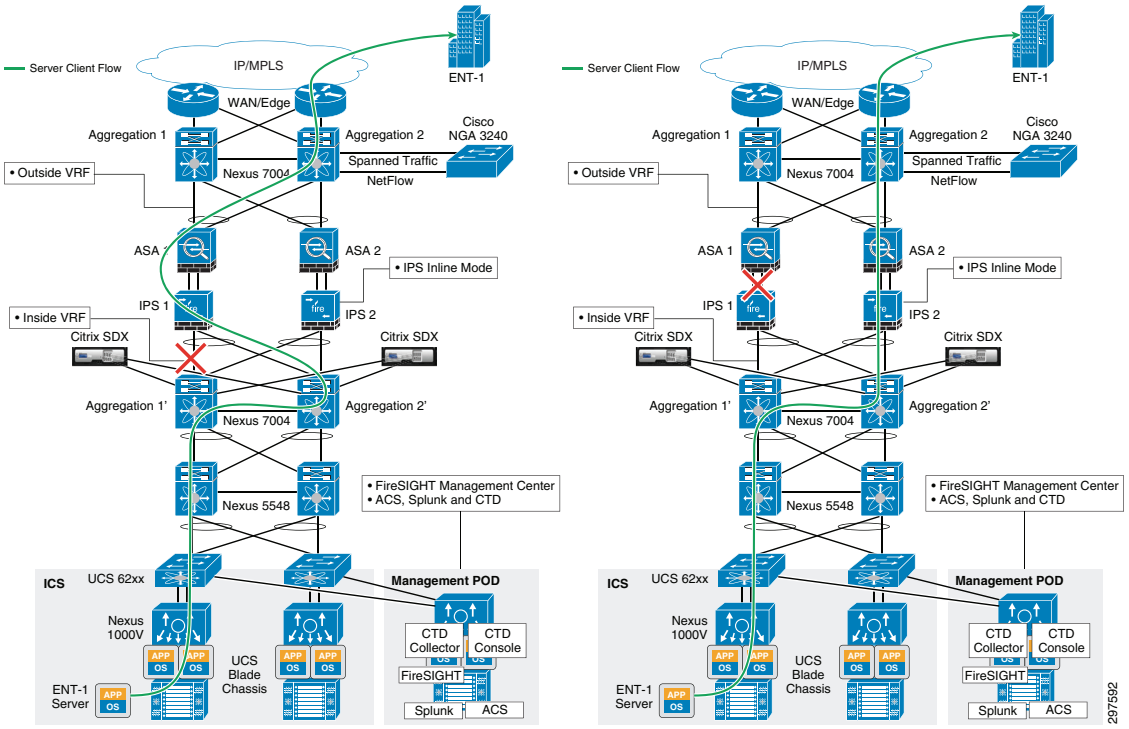


Figure 3-25 Traffic Flows with Various Link Failure



In ASA, link failure detection is based on the weighted average of the number of links. In this configuration, ASA has three links: two data links and one management link. For example, if the weight is set at 50%, at least two links must fail before the ASA firewall appliance can declare the failure, and the aggregation switch eventually reroutes traffic to the secondary path. NGIPS in the secondary path starts picking up new flows in the middle that were dropped from the primary NGIPS. The secondary NGIPS does not drop any flow it captures in the middle, but waits for more packets. If the flows were long-lived and the secondary NGIPS receives more packets, it will build the flows.

If only one physical link failed, either the data or management, there is no traffic rerouting.

Note If only the ASA management link fails, traffic is not rerouted and the SP must fix the link failure. Otherwise, the management capability of the appliance is lost for the duration of failure.

Note Performance of the secondary NGIPS may be impacted if a huge number of long-lived flows were dropped because of primary NGIPS failure.

Traffic Flow

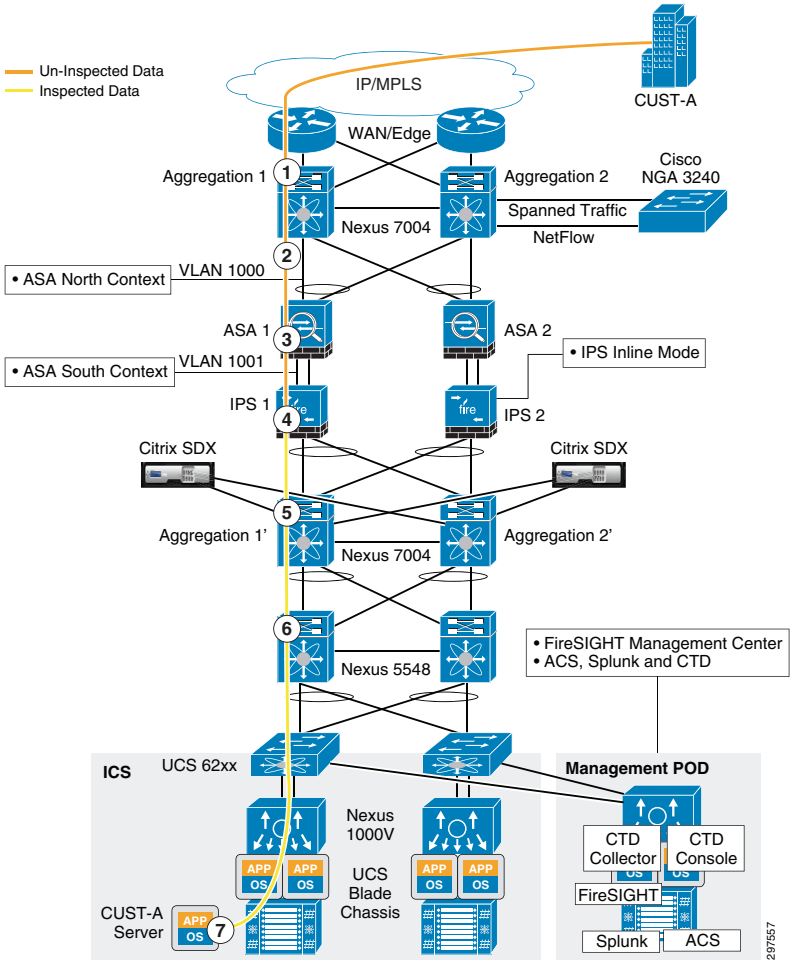
In the following traffic flow example, links between ASA and Nexus 7004 aggregation switches are configured as vPC links, so any such link failure does not impact the traffic flow. If a complete vPC failure, or a failure of any appliance occurs, traffic is rerouted to the secondary path.

1. Packet arrives from the WAN cloud to N7K Agg-1 and is mapped to customer-specific VLAN 1000 (CUST-A-OUTSIDE)
2. Packet destined for the server is sent across the trunk on VLAN CUST-A-OUTSIDE to the ASA-1 context north (outside) interface and ASA applies the firewall policy

3. ASA-1 forwards the packet to N7K Agg-1′ on the south (inside) interface on customer VLAN 1001 (CUST-A-INSIDE)
4. When the packet is forwarded to N7K Agg-1′, NGIPS picks up the flow based on the VLAN tag and inspects the packets based on the configured policy before the packet reaches N7K Agg-1′
5. After being scanned by NGIPS, the packet continues to N7K Agg-1′ with VLAN tag of 1001 (CUST-A-INSIDE)
6. N7K Agg-1’ routes the inspected packet on the Server-VLAN to the server over the trunk to N5K Access-1
7. Packet reaches CUST-A server in the virtual environment

Figure 3-26 shows the traffic flow example.

Figure 3-26 Traffic Flow Example



In this design, physical links from Nexus 7004 aggregation nodes connect to ASA on the outside interface using the port channel. From ASA, the physical links on the inside interface physically connect to NGIPS; from NGIPS, these links are carried out to the Nexus 7004 aggregation nodes on the inside interface to complete vPC connectivity between ASA and Nexus 7004 aggregation nodes.

The NGIPS that is physically between the firewall and aggregation switch is deployed in transparent mode (bump in the wire).

The NGIPS physical port configuration follows:

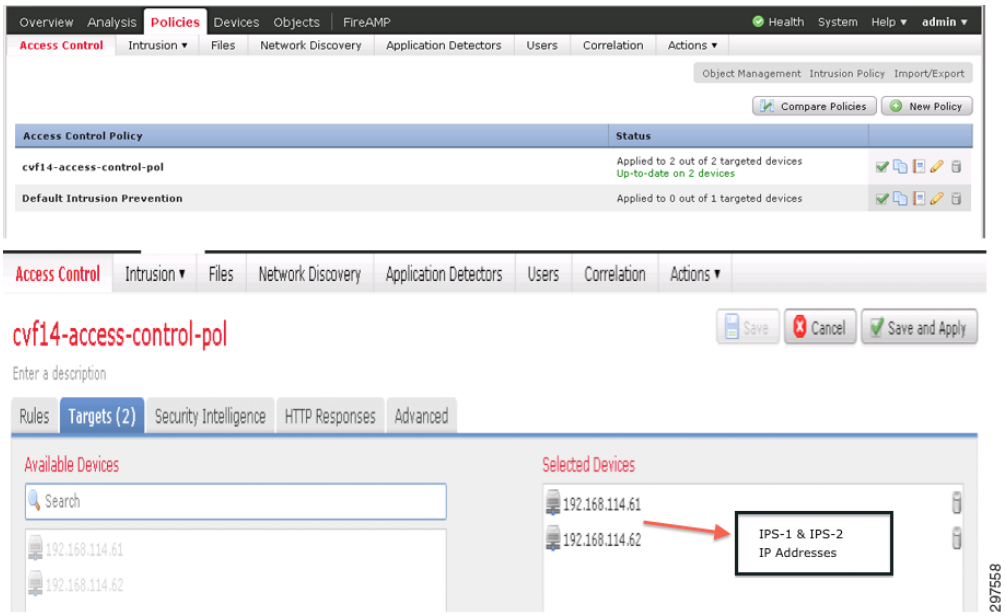
1. Physical Ports 1 – 2 are paired
2. Physical Ports 3 – 4 are paired
3. Physical Port 1 of IPS-1 connects to the northbound ASA -1 first link
4. Physical Port 2 of IPS-1 connects to Agg1′ switch
5. Physical Port 3 of IPS-1 connects to the northbound ASA-1 second link
6. Physical Port 4 of IPS-1 connects to the Agg2′ switch

For example, if port 2 on IPS-1 is down, or the link between port 2 and Agg1′ is down, IPS-1 propagates link failure to port 1 so that ASA knows the first link is down and route traffic to the second link. Similarly, if port 1 is down, IPS-1 propagates the down status toward port 2 so that the Nexus 7004 knows that port is down and routes traffic to Agg2′, which in turn routes the traffic back to the IPS-1 on port 4 (IPS-1 physical port).

When tenant traffic comes into the data center and sent to the FW outside interface the ASA firewall marks the traffic with the associated inside VLAN tag. When the traffic passes through NGIPS, it inspects tenant traffic based on the defined VLAN policies.

As shown in Figure 3-27, IPS-1 and IPS-2 are deployed with identical configurations to support HA. In this mode, FireSIGHT Management Center deploys all configurations on both NGIPS. The SP can configure both NGIPS IP addresses in FireSIGHT Management Center, so whenever new configurations or changes are made, FireSIGHT Management Center downloads the same configurations on both NGIPS. During a failure event, either one of the NGIPS can support the tenants and be able to inspect based on the original policies configured.

Figure 3-27 FireSIGHT Management Center Policies Tab



As shown in Figure 3-27, after creating a policy or after making a change, the user can assign this to one or more devices (NGIPS). The VMDC Cloud Security 1.0 reference architecture specifies two NGIPS; both were added so that changes and new configurations are downloaded to both.

When deploying a single IPS appliance in fail closed mode between the aggregation and access layer, NGIPS appliance failure splits the data center and causes a major data center outage. Deploying multiple NGIPS between the aggregation and access layers supports multiple link failures and a single IPS appliance failure.

Inserting a Single NGIPS at the Aggregation Layer

As shown in Figure 3-28, an NGIPS can be inserted between the aggregation and access layer as a single physical appliance.

Figure 3-28 Inserting a Single NGIPS between the Aggregation and Access Layers

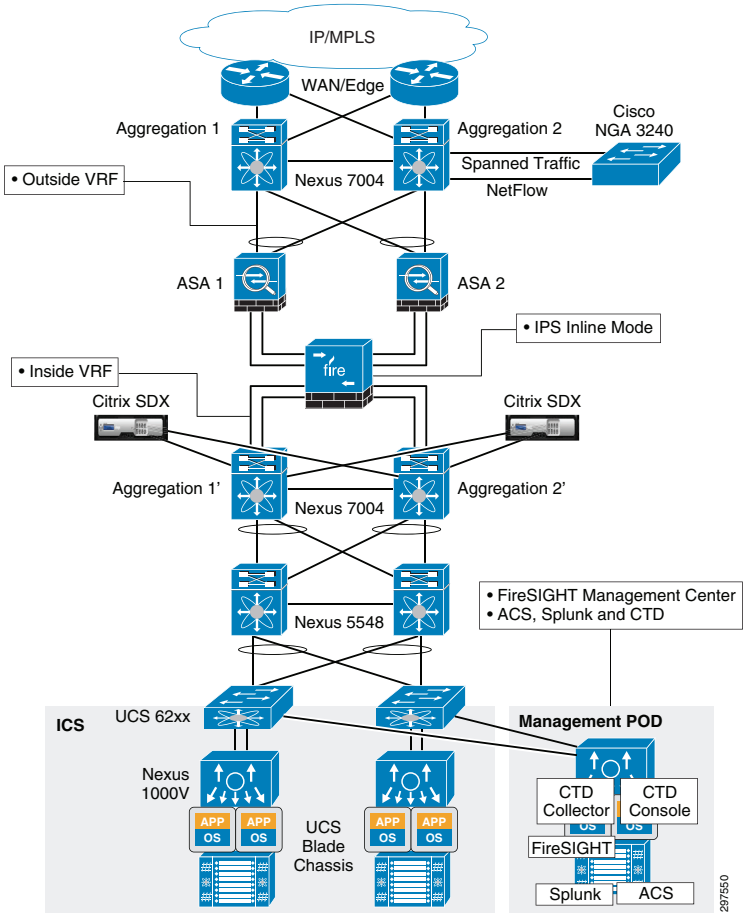


Table 3-6 summarizes the pros and cons of this deployment model.

Table 3-6 Deployment Model Pros and Cons

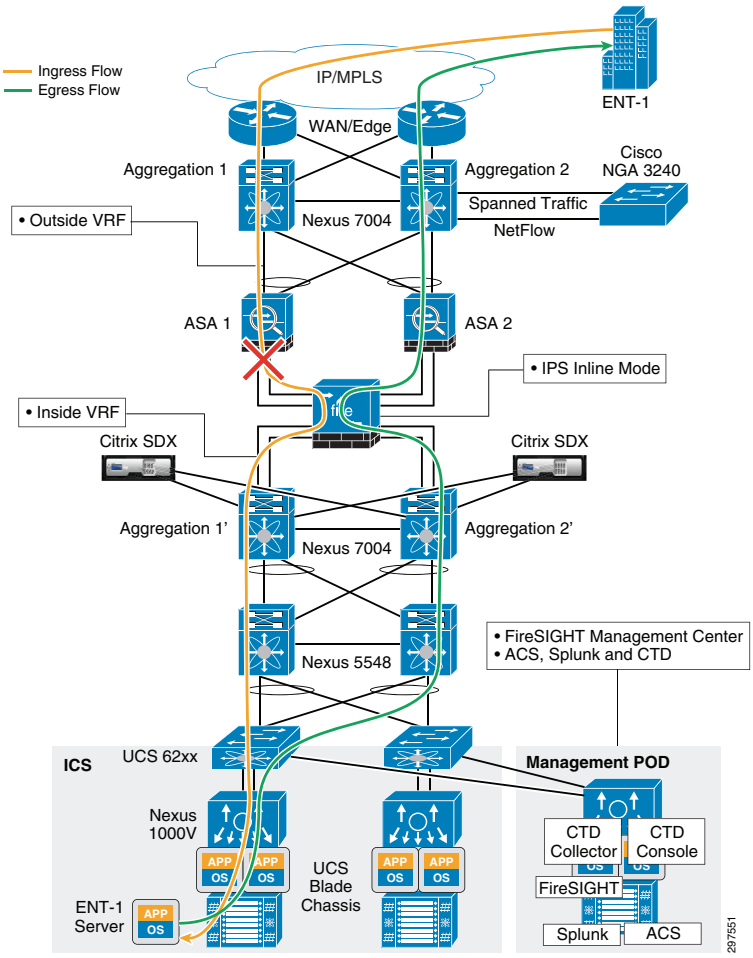
Pros	Cons
Higher Scale than at the access layer. (Required fewer appliances with higher performance)	No High Availability

Table 3-6 Deployment Model Pros and Cons

Pros	Cons
Protect north/south and some east west Traffic	Overall Scale and Performance limited by physical interfaces
No Issue with Asymmetrical traffic	

Deploying a single IPS appliance between the aggregation and access layer resolves the asymmetrical traffic issue as shown in Figure 3-29.

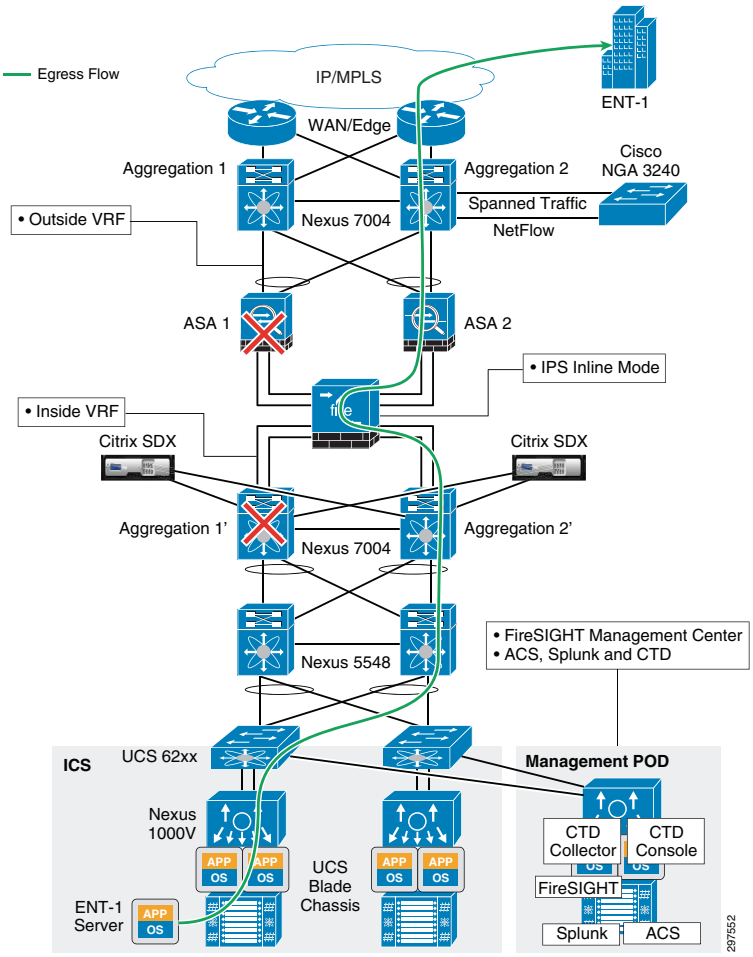
Figure 3-29 Deployment Model Traffic Flows



When traffic flows from outside to inside, it may go through the aggregation switch Agg-1, then pass transparently through NGIPS to access switch 1 and so on towards the server or specific application. On the return path, traffic may go through access switch 2 and then NGIPS and if there is a link failure between ASA-1 and NGIPS, the return traffic goes to ASA-2 to Agg-2 and does not cause any asymmetrical traffic flow issue. This is because there is only one NGIPS appliance between the aggregation and access layers, hence traffic flows from north to south and south to north go through the same NGIPS appliance and there is no asymmetrical flow issue.

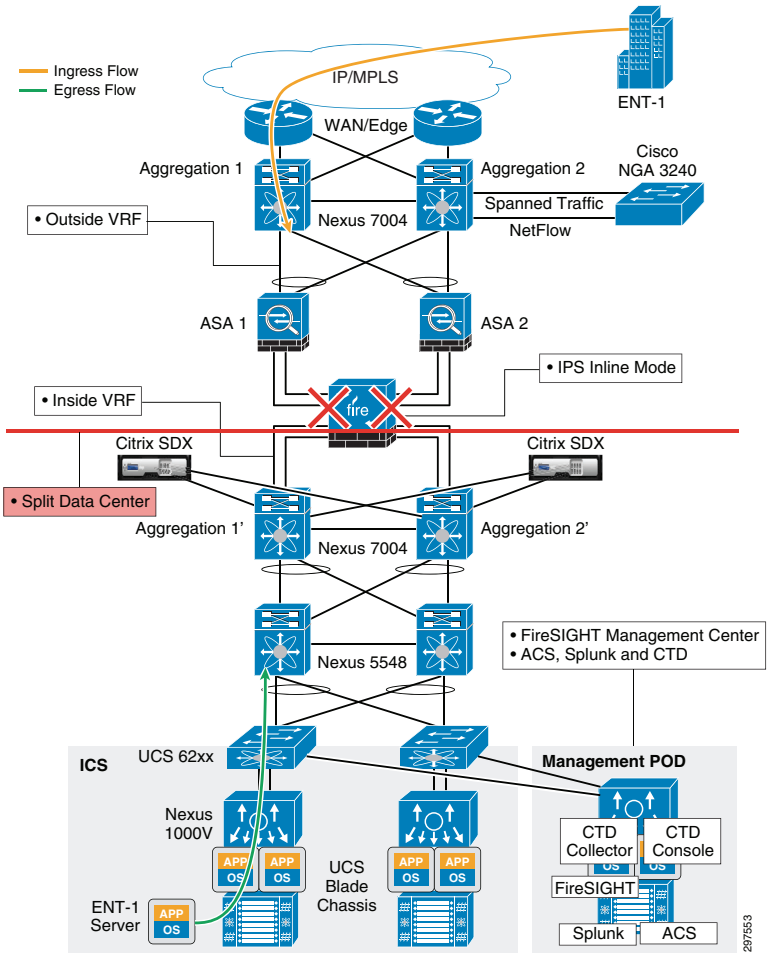
Similarly as shown in Figure 3-30 there is no asymmetrical traffic flow issue through NGIPS even if an ASA firewall or aggregation switch goes down.

Figure 3-30 Firewall or Aggregation Switch Failure



In this deployment model, NGIPS is deployed in fail closed mode, so if the appliance hardware fails, no traffic passes through the appliance. There is no HA when deploying a single appliance. Because NGIPS sits inline physically between the aggregation and access layers, an NGIPS hardware failure causes a major outage and north-south traffic is completely disconnected, causing a major disaster in the data center. This design can sustain a single link failure, but failure of the appliance hardware causes a complete loss of cloud services, as shown in Figure 3-31. This splits the data center and all services are down until the NGIPS appliance recovers.

Figure 3-31 NGIPS Appliance Failure

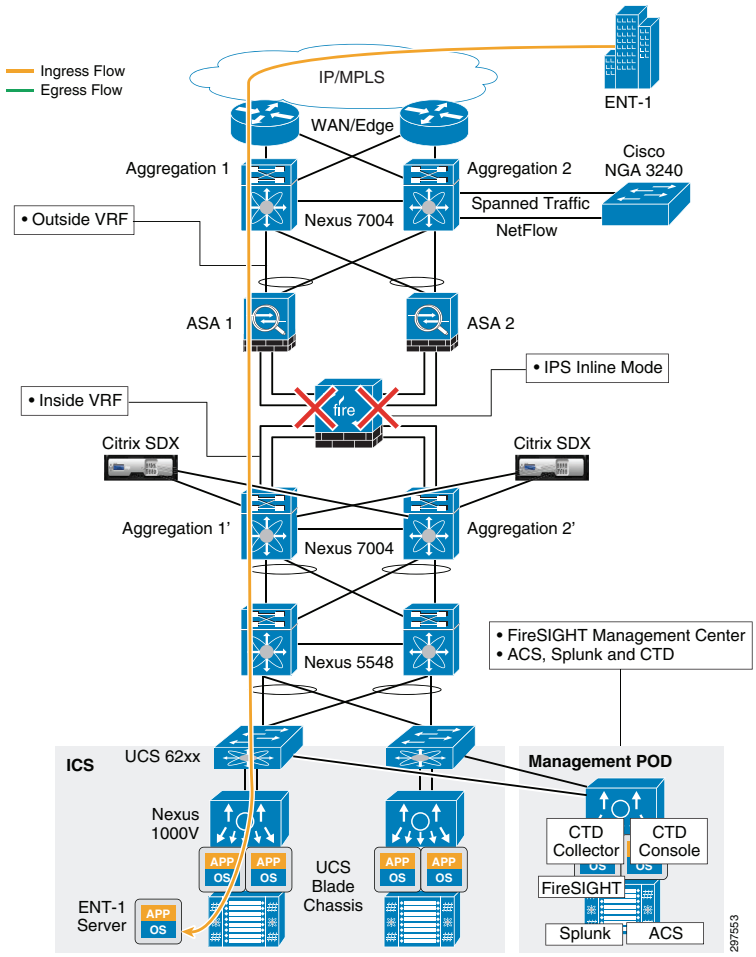


Note Recommendation is to inspect traffic at all times, hence fail open mode is not tested in this release.

On the other hand, if a single NGIPS is deployed in a fail open mode, hardware failure of the appliance may not cause a complete data center disaster as shown in Figure 3-32.

However in fail open mode the cloud services may not get impacted, but NGIPS passes traffic without any inspection which may impose security threat to the entire data center.

Figure 3-32 Appliance Failure in Fail Open Mode

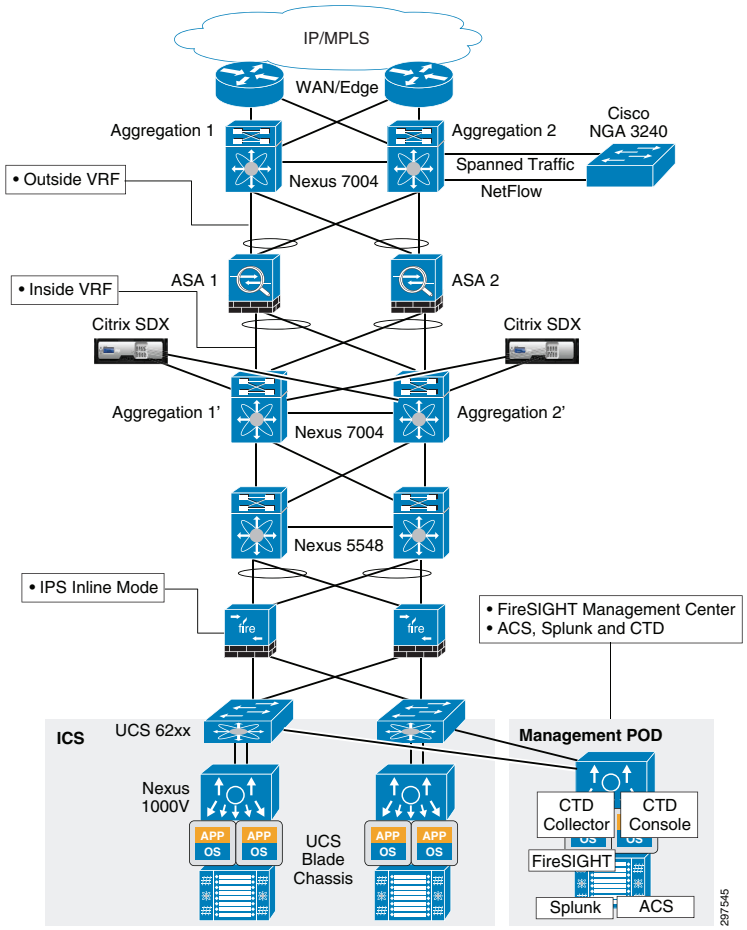


Note Designs in which a single component failure causes a major outage are never recommended, especially in multi-tenant environments. In multi-tenant environments, the architecture should be able to sustain any single component failure or multiple link failures in the data center.

Inserting NGIPS at the Access Layer

NGIPS can be inserted at the access layer as shown in Figure 3-33:

Figure 3-33 Inserting NGIPS at the Access Layer



NGIPS is deployed in transparent mode, as a bump in the wire, and is in active or inline mode. In this design, NGIPS is deployed at the access layer, or between Nexus 5000 access switches and Fabric Interconnect.

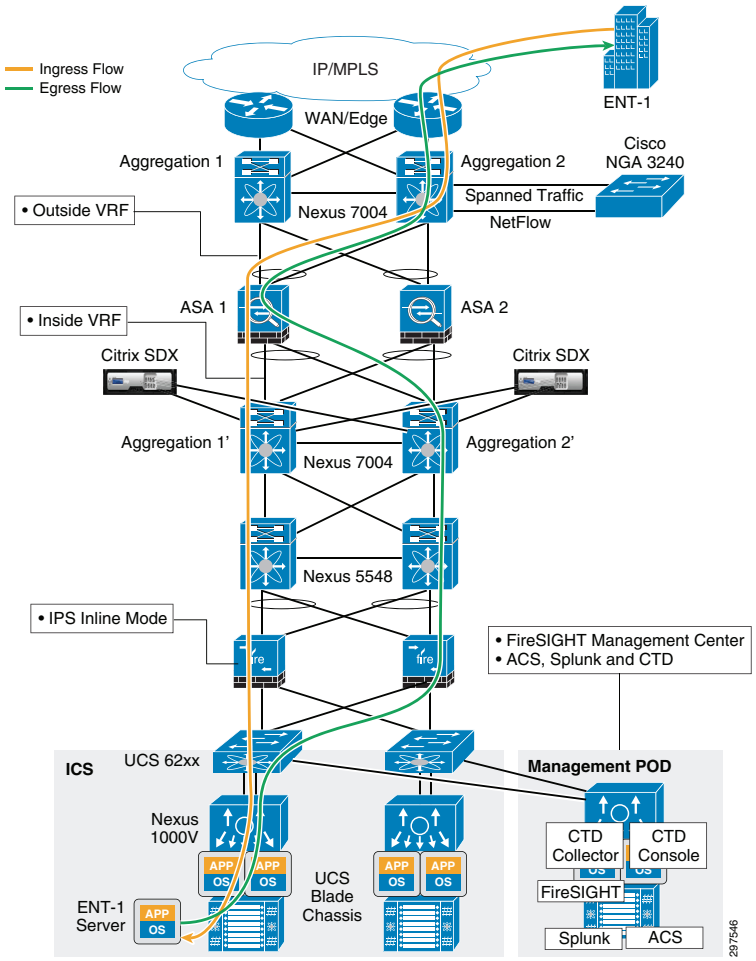
Table 3-7 summarizes the pros and cons of this deployment model.

Table 3-7 Deployment Model Pros and Cons

Pros	Cons
Close to the asset i.e. applications and server	Not Scalable. Require a pair of NGIPS per Compute Pod (Vblock or FlexPod)
Protect north/south and some east west Traffic	Asymmetrical traffic issue
High Availability	

Figure 3-34 shows the ingress and egress data flows.

Figure 3-34 Ingress and Egress Data Flows



As shown in Figure 3-34, ingress traffic gets to the server through aggregation 1 and access switch 1 and fabric interconnect 1 to the respective server. The return path from server depends upon the hashing algorithm of UCS – FI, which may return the traffic to either N5K-1 or N5K-2.

Due to this internal hashing mechanism of UCS-FI, egress traffic may get to N5K-2 through IPS 2. This creates an asymmetrical traffic flow in which some incoming packets may flow on one side and some incoming packets may flow on the other side. In the preceding example, incoming traffic passes through IPS-1, which picks up the flow, but on the return path egress traffic flows through IPS-2.

This design can sustain a single NGIPS appliance failure and multiple vPC link failures. If an NGIPS appliance fails, traffic is directed to the second IPS-2, which tries to pick up the traffic at mid-flow. If the flow is long enough, NGIPS builds the flow using the next few packets. If flows are short-lived, the original flows which were active on IPS-1 are lost. This happens for only a very short period before new flows are captured by the second IPS-2.

Inserting NGIPS at the Data Center Edge

Figure 3-35 shows the placement of multiple NGIPS between the data center edge or WAN edge and data center aggregation layer.

Figure 3-35 Inserting NGIPS between the Data Center Edge and Data Center Aggregation Switches

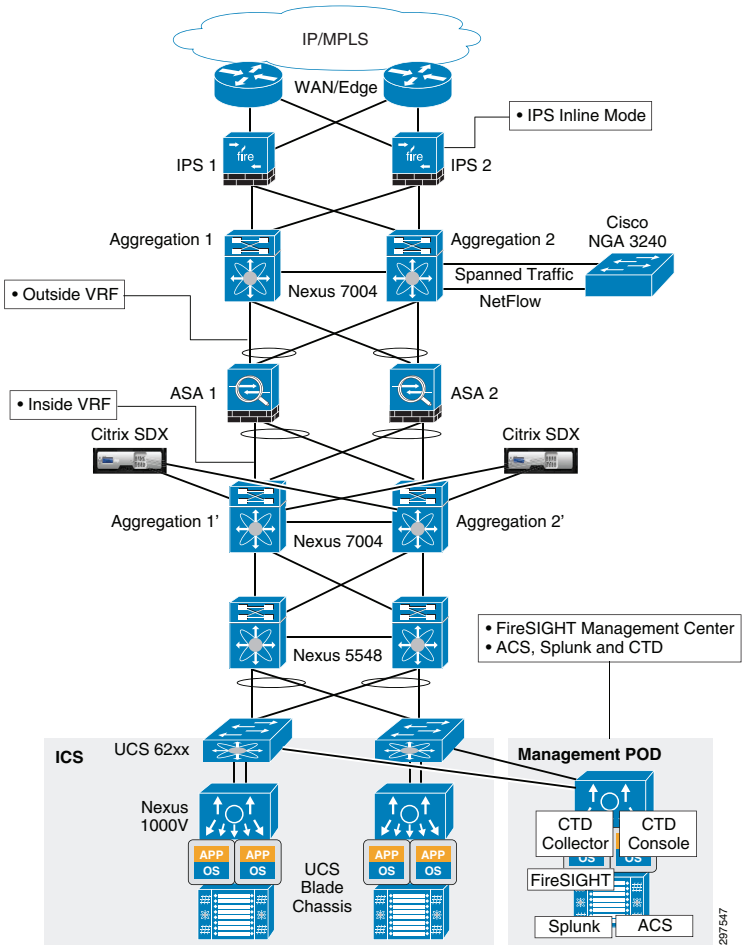


Table 3-8 summarizes the pros and cons of this deployment model.

Table 3-8 Deployment Model Pros and Cons

Pros	Cons
Higher Scale	Asymmetrical traffic Issue
Protect only north/south Traffic	Far from protected Assets
	Capture Unwanted traffic too

When deploying NGIPS between the data center edge and the data center aggregation layer, all traffic goes through NGIPS.

In this design, NGIPS captures all the traffic coming into the data center, so NGIPS also processes some unwanted traffic. For example, if unauthorized users or devices try to access the data center, NGIPS inspects their traffic, too, and wastes processing power and may create false alarms. On the other hand, if NGIPS is deployed behind the data center firewall, it does not see unauthorized user or device traffic and so uses less processing power.

This design can sustain a single NGIPS failure. Traffic fails over to the secondary NGIPS with minimal disruption as shown in Figure 3-36 and Figure 3-37.

Figure 3-36 Ingress Traffic Flow

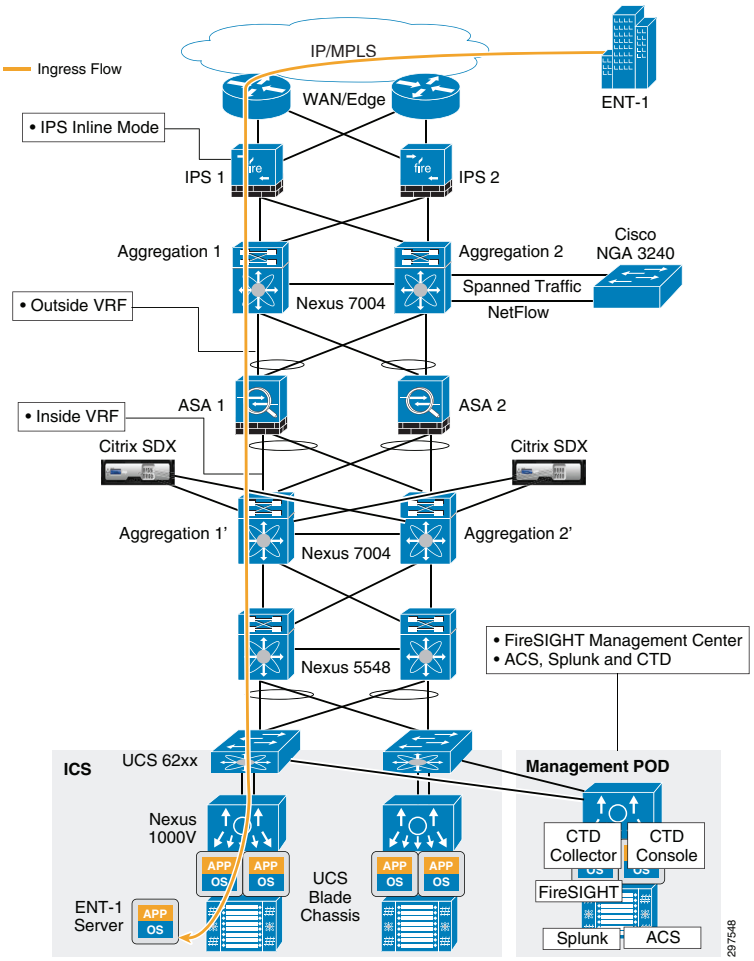
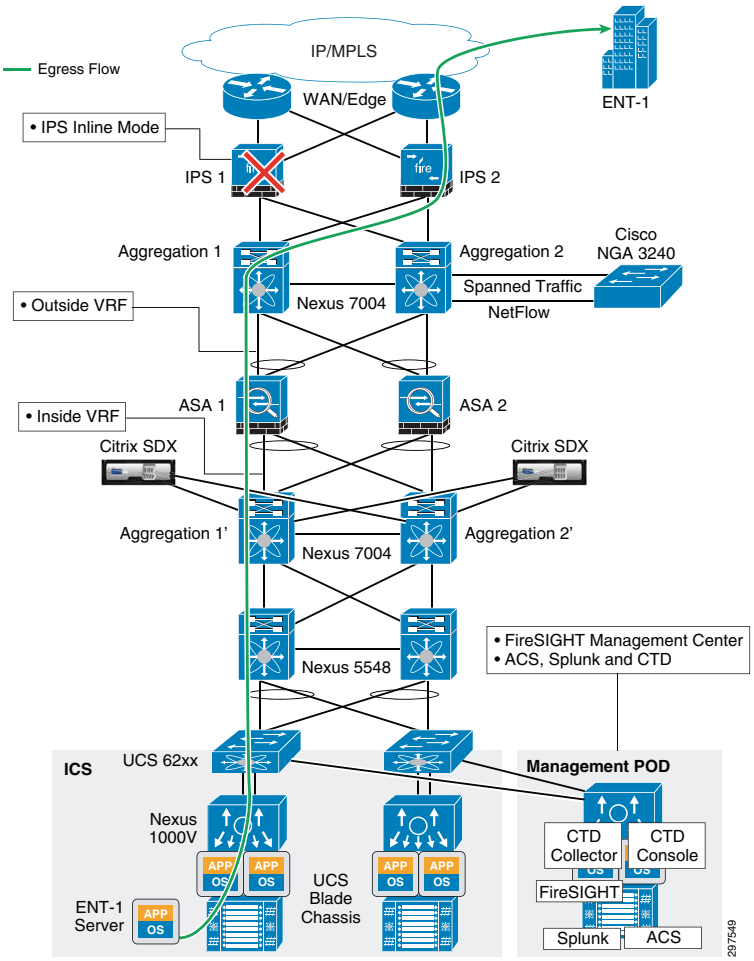


Figure 3-37 Egress Traffic Flow



Deploying the Management Network

The management network can be deployed by using an out-of-band (OOB) access to manage devices in the data center. To accomplish OOB, dedicated management ports are connected to a dedicated OOB network that hosts management and monitoring services. This section describes the general outline and best practices for deploying a management network. Details of the deployment of the management network used in this solution will be provided in the implementation guide.

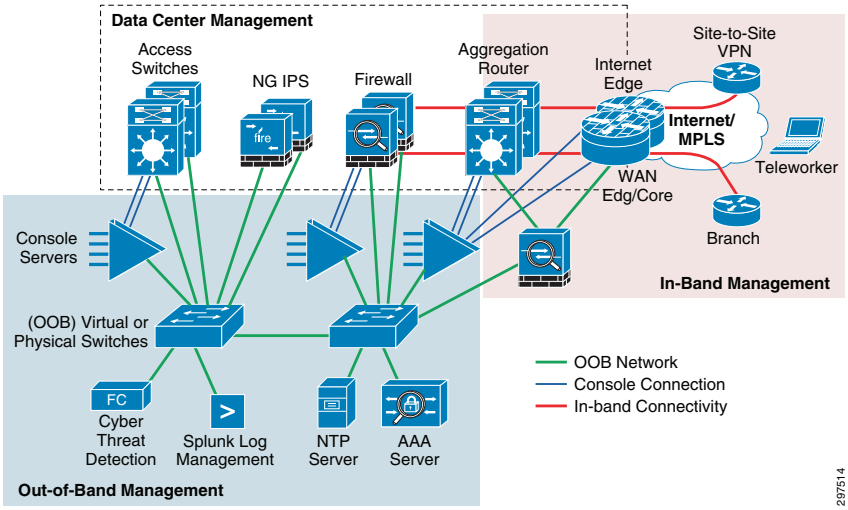
The OOB network segment hosts console servers, network management stations, authentication, authorization, accounting (AAA) servers, analysis and correlation tools, Network Time Protocol (NTP), File Transfer Protocol (FTP), Syslog servers, network compliance management, and any other management and control services.

The management network deployment should use the following best practices:

- Provide isolation of the OOB network from the network infrastructure
- Enforce access control of all managed devices
- Separate different types on management traffic into separate subnets

In the OOB infrastructure, using dedicated switches, firewalls, and VLAN subnets implements separation between data and management networks,.These dedicated appliances are in addition of the network infrastructure described within the VMDC architecture. Optionally as shown, one can allow for in-band (IB) management of Internet facing devices, where management access is achieved by using links used for user data flows. The logical topology of the management network is shown in Figure 3-38.

Figure 3-38 Data and Management Network Separation



Management Network Considerations

The management plane carries NetFlow traffic, along with NetFlow Secure Event Logging (NSEL) traffic between Adaptive Security Appliance (ASA) and NetFlow Generation Appliance (NGA) appliance and the Cisco Cyber Threat Defense (CTD) collector. It is a best practice to keep management traffic on a separate subnet, and we recommend using a separate subnet for management traffic for the physical appliances.

When deploying switches and firewalls in the OOB network, consider the following:

- The OOB components such as AAA servers, or log management systems can be either physical appliances or virtual machines. If virtual machines (VMs) host Cisco CTD or Splunk applications, one can leverage Nexus1000V to provide connectivity to the OOB network. One must use separate VLANs and port profile configurations in Nexus 1000V virtual switches to achieve management separation for management VLANs from the rest of the network.
- If In-band management connectivity is configured for core or aggregation routers, you must separate management ports using a firewall to reduce the risk of unauthorized access to the entire management domain.
- Authenticate and authorize access to devices using AAA.
- Use HTTPS and SSH for device access.

Deploying Network Time Protocol Services in the Management Network

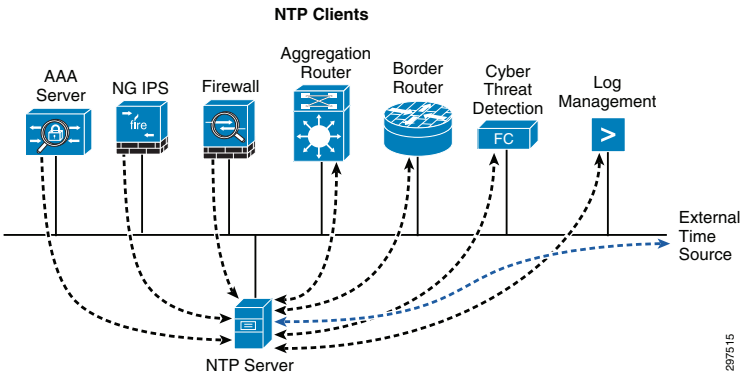
Time synchronization using NTP for network and security devices is critical for threat correlation, event analysis, and log management. NTP traffic also uses the OOB management network to communicate with time servers.

When deploying NTP in the OOB management network, consider the following:

- Deploy a hierarchical NTP design rather than a flat design. Within this framework, all devices within the data center are synced with a local NTP server, and that server is then synced to an external time-source. Hierarchical designs are preferred because they are highly stable, scalable, and provide the most consistency.
- Use a common time zone throughout the infrastructure to facilitate event analysis and correlation.
- Control which clients and peers can talk to an NTP server.
- Enable NTP authentication.

In this design, routers and switches can be configured as clients having a client/server relationship with internal time servers in the OOB management network. The internal time servers are synchronized with external time sources as shown in Figure 3-39.

Figure 3-39 Time Server Synchronization with External Time Source



Authentication and Role-Based Access Control

Network infrastructure devices often provide a range of different access mechanisms, including console and asynchronous connections, as well as remote access based on protocols such as Telnet, rlogin, HTTP, and SSH. Some mechanisms are typically enabled by default with minimal security associated with them; for example, Cisco IOS software-based platforms are shipped with console and modem access that is enabled by default. For this reason, each infrastructure device should be carefully reviewed and configured to ensure only supported access mechanisms are enabled and that they are properly secured. The key measures to securing both interactive and management access to an infrastructure device are as follows:

- Restrict device accessibility
  - Limit the accessible ports and restrict the permitted communicators and the permitted methods of access.
- Present legal notification

  - Display legal notice developed in conjunction with company legal counsel for interactive sessions.
- Authenticate access
  - Ensure access is only granted to authenticated users, groups, and services.
- Authorize actions
  - Restrict the actions and views permitted by any particular user, group, or service.
- Ensure the confidentiality of data
  - Protect locally stored sensitive data from viewing and copying.
- Log and account for all access
  - Record who accessed the device, what occurred, and when for auditing purposes. Implementing Authentication, Authorization and Accounting (AAA). AAA is an architectural framework for configuring the following set of independent security functions in a consistent, modular manner:

    Authentication—Enables users to be identified and verified prior to them being granted access to the network and network services.

    Authorization—Defines the access privileges and restrictions to be enforced for an authenticated user.

    Accounting—Provides the ability to track user access, including user identities, start and stop times, executed commands (such as command-line interface (CLI) commands), number of packets, and number of bytes.

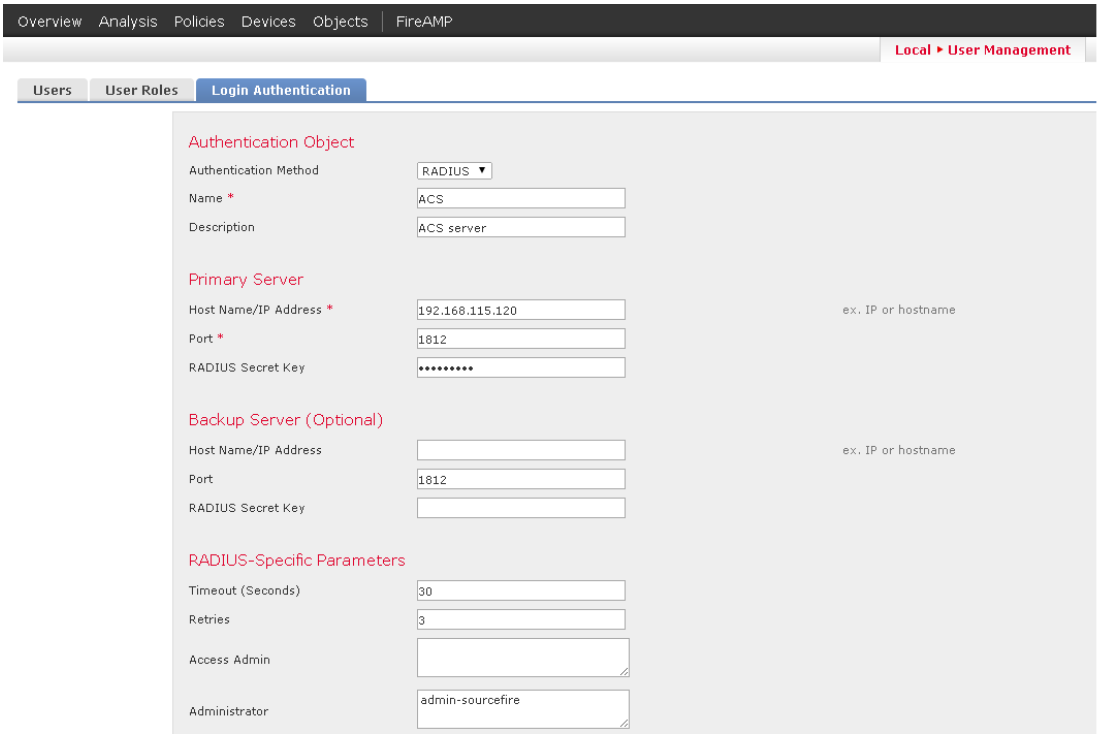
In this solution Cisco Access Control System (ACS) in conjunction with Active Directory is leveraged to implement password protection, Role Based Access and AAA services. In addition ACS provides detailed reports on events such as: who accessed a network and when; who failed to access which devices; what command did they execute; details on device configuration changes. Detailed reports on these events as well as secure auditing, is required for regulatory and compliance efforts. More information on deploying and managing ACS access policies and identity roles can be found at:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-5/user/guide/acsuserguide/introd.html

In addition to the existing network infrastructure devices; the newly introduced FirePOWER and Cyber Threat Defense security appliances offer a number of configuration options to implement access control.

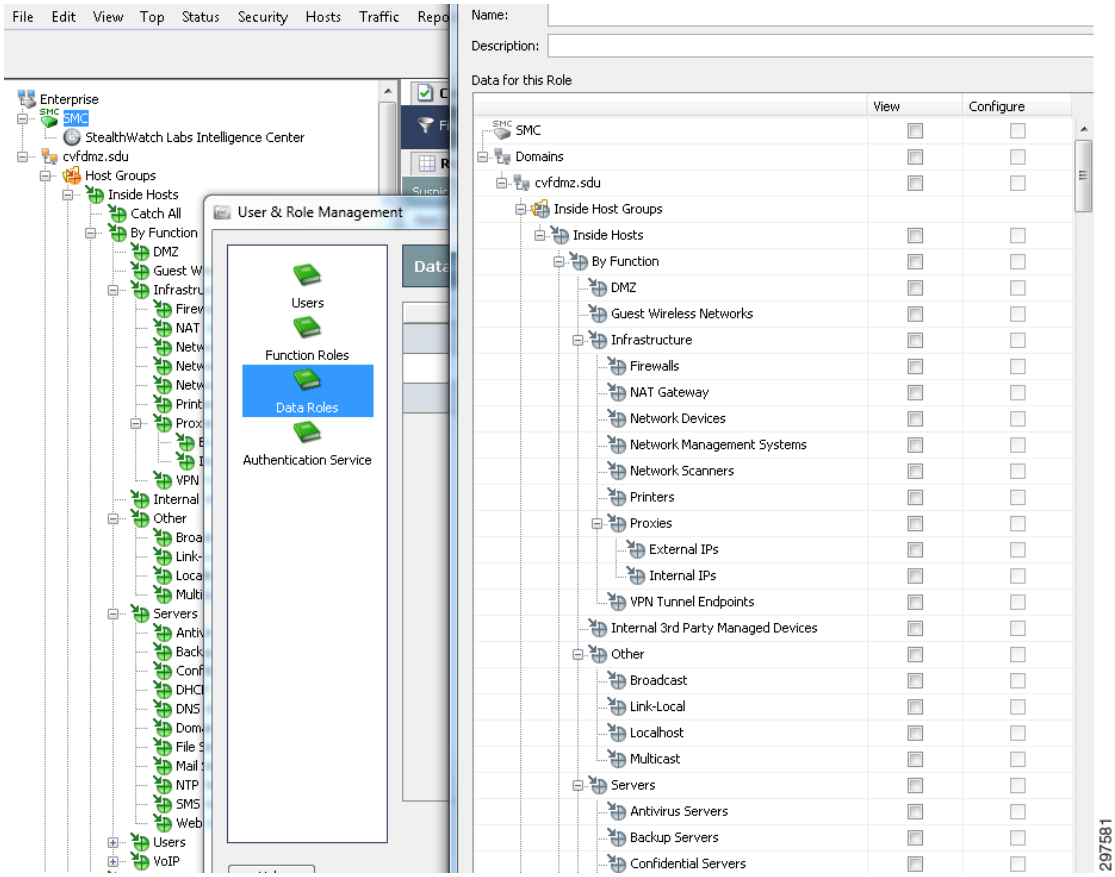
FirePOWER authentication is performed through active directory. Configuration can be done under “System/User-Management” pane, where users, user-roles and login authentication parameters can be set. Various predefined user roles are available and can be assigned to different users. FirePOWER can point to the ACS server for authentication under the login-authentication page as shown in Figure 3-40.

Figure 3-40 Login-Authentication Page



In Cisco CTD, the user can set management parameters under the configuration/user management pane including setting up other users, functional roles and authentication service. Similar to the FirePOWER appliance, there are predefined functional roles that can be leveraged, such as Configuration Manager, or Security Analysts. Custom-made roles can also be configured. These functional roles define what information can be viewed. In addition the data roles define what parameters can be viewed as well as configured. Figure 3-41 shows the data role configuration screen within the Cisco CTD's SMC console, where custom-made roles can be configured

Figure 3-41 Data Role Configuration Screen



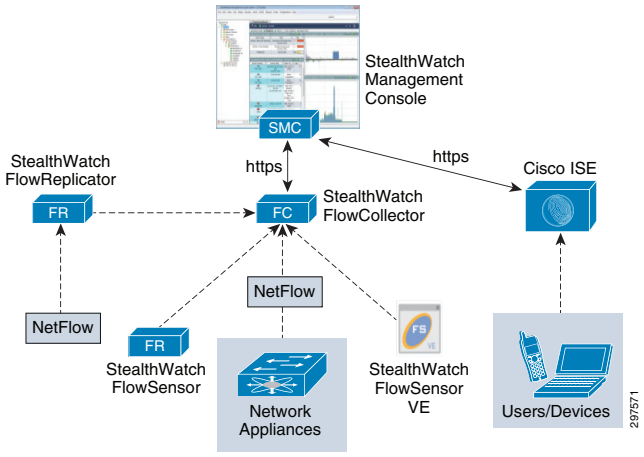
Integrating Cisco Cyber Threat Defense

Cisco Cyber Threat Defense (CTD) uses network device telemetry to provide deep, complete visibility across the network core, enabling security operators to understand and use network traffic details to discover anomalies. Deploying Cisco CTD across networks can provide information and visibility to support security operators in a variety of threat detection tasks, including:

- Data loss detection
- Network reconnaissance of internal networks
- Monitoring the spread of malware in internal networks
- Botnet command and control channel detection in internal networks

Figure 3-42 shows the main components of Cisco CTD.

Figure 3-42 Cisco CTD Solution Components



In this solution, the Cisco CTD component are:

- **FlowCollector**—A virtual appliance that aggregates and normalizes NetFlow and application-type data collected from Cisco Nexus Series switches, Cisco Adaptive Security Appliance (ASA) firewalls, and Cisco NetFlow Generation Appliance (NGA)
- **StealthWatch Management Console (SMC)**—A virtual appliance that aggregates, organizes, and presents FlowConnector analyses using graphical representations of network traffic, customized summary reports, and integrated security and network intelligence for drill-down analysis

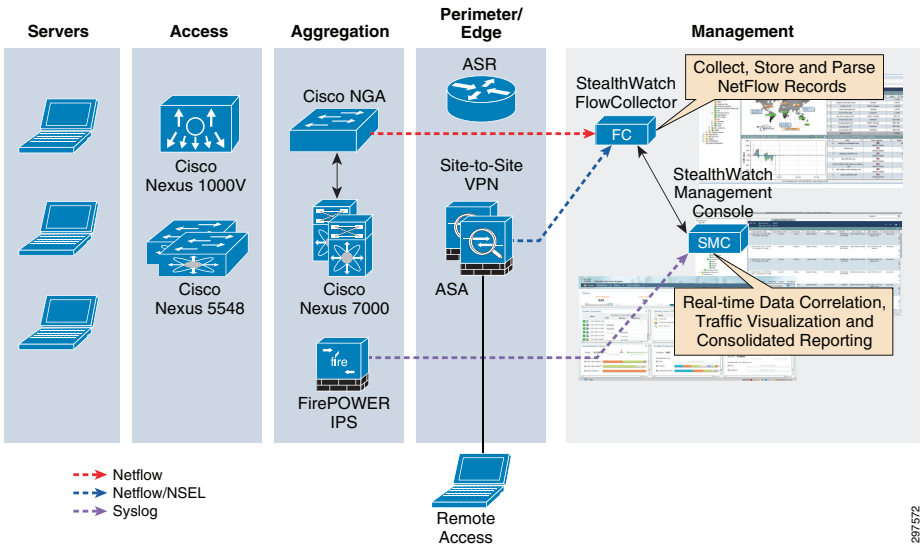
Note Other Cisco CTD components shown in Figure 3-42, such as FlowSensor, are optional and are not deployed in this version of this solution.

Architecture

Cisco CTD uses network traffic telemetry from ASA 5585-X Series Next Generation Firewalls and NGA, which converts raw traffic spanned from Nexus 7000 Series switches to NetFlow records. These appliances export NetFlow records to FlowCollector, which forwards them to SMC. SMC provides centralized management for all netflow-enabled appliances, and provides real-time data correlation, visualization, and consolidated reporting.

Figure 3-43 shows the high-level Cisco CTD system architecture.

Figure 3-43 FCTD System Architecture



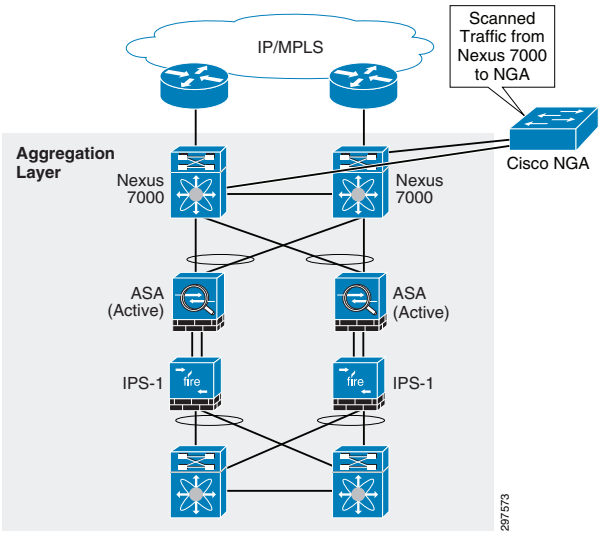
Cisco CTD can be configured to translate Syslog messages from FirePOWER generated by Intrusion events in its database and reporting structure.

Deploying Exporters

The ASA implementation of NetFlow, called NetFlow Security Event Logging (NSEL), enables specific high-volume traffic events to be exported from the security appliance more efficiently and in a more scalable way than standard Syslog logging. NSEL can be configured in separate contexts on ASA to support per-tenant visibility. After Cisco CTD receives NSEL records from each ASA context, Cisco CTD populates multiple contexts in its exporter-tree database. Exporters can also be manually configured using a Cisco CTD configuration menu.

In large data centers, generating NetFlow at high rates can be challenging. To address this, NGA converts raw high-rate data traffic that is spanned from Nexus 7000 Series switches, and converts it to NetFlow Version 9 traffic. NGA has four 10 Gigabit Ethernet (10 GbE) monitoring interfaces and up to four independent flow caches and flow monitors. Two 10 GbE ports are used to receive Nexus 7000 data. Strategically placing the NGA in the aggregation layer provides effective traffic monitoring in the data center, and provide additional statistics for traffic leaving the data center. Figure 3-44 shows the NGA deployment.

Figure 3-44 NGA Deployment



When deploying NGA and ASA to export NetFlow data, NSEL and NetFlow Version-9 does not export identical object fields. Understanding what each device exports helps to develop end-to-end strategies for obtaining a complete network visibility. This is described in more detail in Event Correlation and Data Analysis, page 4-9.

Note The following documents describe the fields supported in NSEL and NGA and further information on various deployment options and performance of NGA.

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/system/netflow/netflow.pdf
- http://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/threat-defense/cyber_threat_defense_design_guide.pdf
- http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/netflow-generation-3000-series-appliances/white_paper_c11-708294.html

Deploying StealthWatch FlowCollectors

StealthWatch FlowCollectors deployments can be distributed or centralized. In distributed deployments, FlowCollectors are deployed at multiple locations and are usually placed close to the source producing the highest number of NetFlow records. In a multi-tenant environment, we recommend the following best practices:

- Separate FlowCollectors can be used for tenants having overlapping IP addresses. Each FlowCollector should be placed in a separate domain in the SMC domain tree. This enables separation and simplifies data analysis for tenants that use overlapping IP addresses. Tenant-specific NetFlow records are configured and exported in each ASA context.
- Multiple tenants can export NetFlow data to the same collector. In this scenario, ensure that the total number of exported flows do not exceed FlowCollector capacity.
- Use a separate FlowCollector to collect NetFlow records from NGA. Because NGA exports aggregated traffic from all tenants, ensure that this FlowCollector has sufficient capacity to collect state data on all conversations without purging active records before reaching the idle-time threshold.

- When firewalls are deployed in the management network, appropriate ports and services must be enables to ensure correct communication and operation of the various Cisco CTD components. Table 3-9 summarizes the required services:

Table 3-9 Cisco CTD Component Ports and Services

Client	Server	Port	Comment
SMC	FlowCollector	TCP/443	HTTPS
SMC	Servers in Management Network	UDP/161	SNMP
		UDP/123	NTP
		TCP/25	SMTP
		UDP/53	DNS
		UDP/162	SNMP-Trap
		UDP/514	Syslog
Exporters	SMC	UDP/2055	Netflow records
Exporters/SMC /Collectors	ACS/Radius Server	UDP/1812/1813	Authentication

For more detailed information about required services, refer to http://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/threat-defense/cyber_threat_defense_design_guide.pdf.

These recommendations limit NetFlow overhead and provide per-tenant visibility even if tenants use overlapping IP addresses. This deployment model can support the use separate FlowCollectors for high-end network container types, and another FlowCollector to aggregate NetFlow records from multiple lower-end tenants.

Performance is another important design consideration. The following important factors should be considered:

- **Exporter Count**—the number of exporting devices that each FlowCollector can accept.
- **Data Rate**—the flows per second (fps) rate that the FlowCollector receives.
- **Host Count**—the number of hosts inside and outside the network for which the FlowCollector can maintain state. We recommend that the number of inside hosts not exceed 60% of the host count value.
- **Flow Storage**—the amount of granular flow data storage required for a particular network location.

Traffic throughput (Gigabit per second, or Gbps) has no direct bearing on exported fps; the only measure that directly impacts throughput is the number and rate of flows passing through a device. For example, a high-volume (1 Gbps) flow could pass through a port, resulting in an fps less than one. In contrast, many small-volume flows could pass through a port, resulting in low total throughput but high fps (4000 fps with a total throughput of 100 Mbps, for example).

Table 3-10 summarizes the FlowCollector VE system requirements:

Table 3-10 FlowCollector VE System Requirements

fps	Exporters	Hosts	Reserved Memory	Reserved CPUs
Up to 4,500	Up to 250	Up to 125000	4 GB	2
Up to 1,5000	Up to 500	Up to 250,000	8 GB	3

Table 3-10 FlowCollector VE System Requirements (continued)

fps	Exporters	Hosts	Reserved Memory	Reserved CPUs
Up to 22,500	Up to 1000	Up to 500,000	16 GB	4
Up to 30,000	Up to 1000	Up to 500,000	32 GB	5

For more information in about performance design considerations, refer to http://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/threat-defense/cyber_threat_defense_design_guide.pdf.

CHAPTER 4

End-to-End Visibility

One of the main challenges facing internal network security is providing visibility of data streams flowing through every part of a network. Because there is simply no central location where data can be gathered, visibility by its nature operates on a distributed paradigm. An effective solution must be able to collect data from the entire network, then translate and interpret the collected information in a way that maximizes threat detection.

Within this solution, visibility is achieved by implementing Cisco CTD, FirePower appliance, Splunk and NGA. Table 4-1 shows the different roles of these components that facilitate end-to-end visibility.

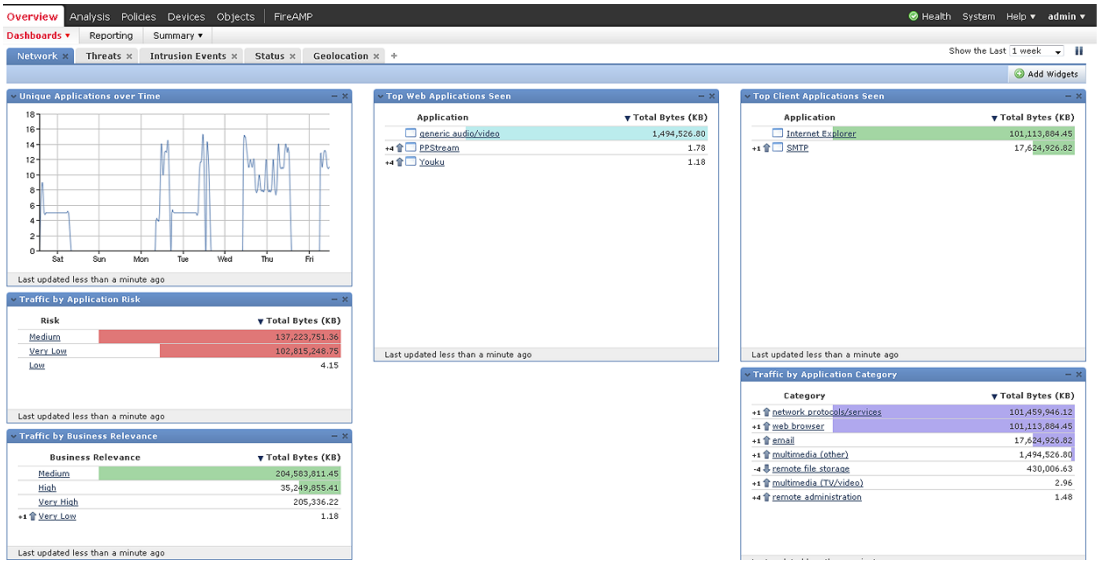
Table 4-1 Visibility Leveraging VMDC Components

Network Components	Coverage Area	Feature Description
Network Intelligence (Routers/Switches/Firewalls)	L1-L4	• Flow events • Appliance Alarms • Topology and Routing Changes
Malware Events (FirePOWER)	Files	• Malware Detection • File Types • File Transfers
Anomaly Detection Events (CTD)	DDoS/Bots	• DDos/Reconaisence/Bot Detection
Threat and Security Events (FirePOWER/FireSIGHT)	L4-L7	• Correlation and Security • Intelligence Events • Hosts/Users • OS Events
Intrusion Events (FirePOWER)	L4-L7	• IDS/IPS Snort Generated Events

Visibility using FireSIGHT

FirePOWER can be configured to detect security threats using various network objects. Configured FirePOWER appliances, report top web and client applications and can help detect threats that hide in obscure applications. Tracking unique applications over time, and traffic applications by risk, can also help detect attacks, as shown in Figure 4-1.

Figure 4-1 FirePOWER Network Monitoring



FirePOWER Intrusion Event Monitoring

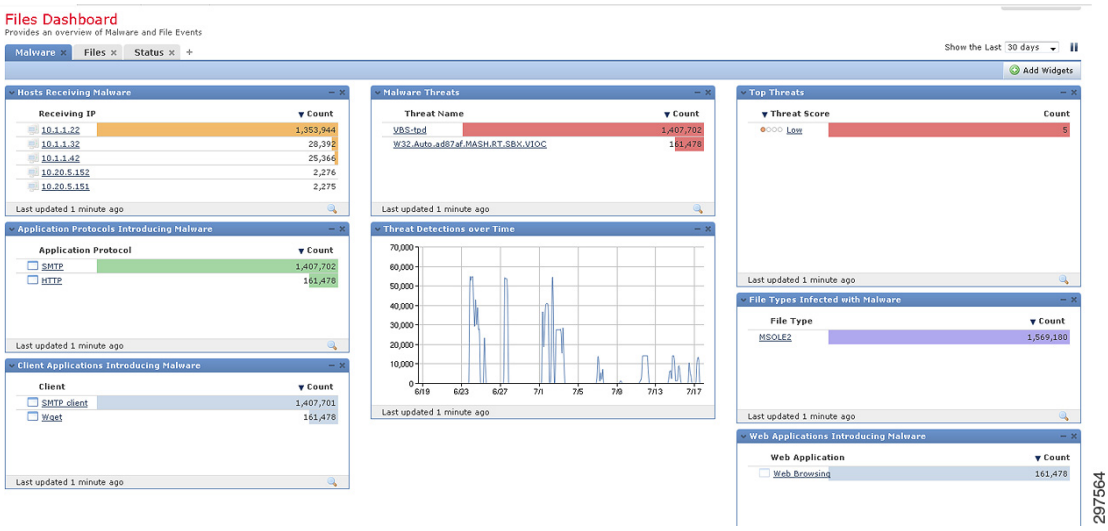
Intrusion monitoring of over time provides information about dropped intrusion events, top targets and attackers, and total events by application protocol. This information can be used to mitigate and prevents intrusion events over time (Figure 4-2).

Figure 4-2 FirePOWER Intrusion Event Monitoring

FirePOWER Malware Event Tracking

FirePOWER can be configured to display malware files, examined and captured files, and network file trajectories. Tracking malware enables quick responses to malware in the data center (Figure 4-3).

Figure 4-3 FirePOWER Malware Event Tracking

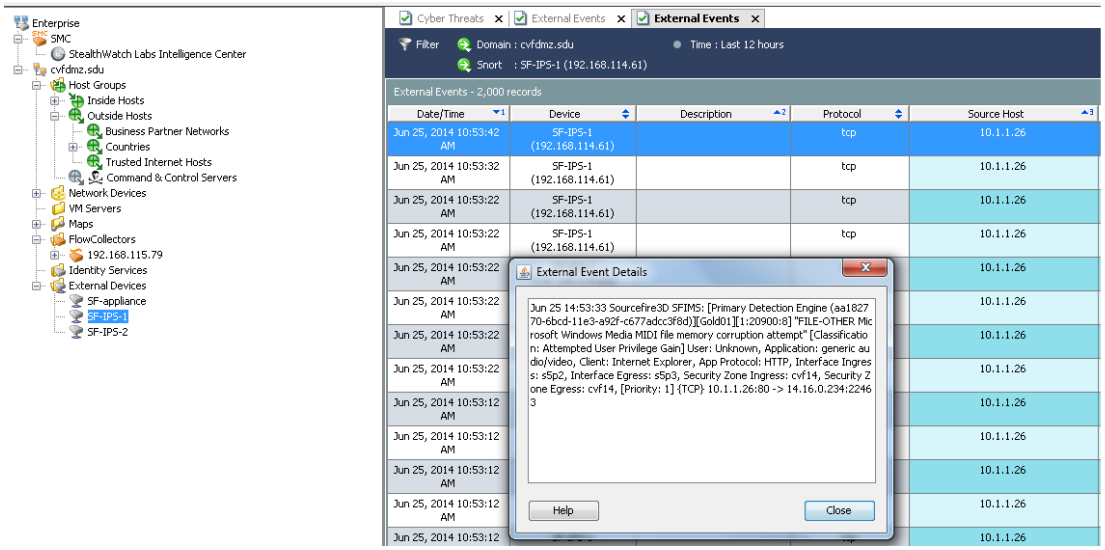


Integrating Intrusion and Malware Events from FirePOWER Appliances into Cisco CTD

FirePOWER appliances can be configured to generate Syslog messages when detecting intrusion and malware events. These Syslog messages can be forwarded to Splunk log management and Cisco CTD. Cisco CTD will translate these syslog messages and integrate those events within its own database.

FirePOWER and Cisco CTD integration provides a more complete, unified view of the network. As shown in Figure 4-4, FirePOWER events are shown under external devices, within SMC's dashboard, where intrusion events are populated and linked under a FirePOWER NGIPS appliance.

Figure 4-4 FirePOWER NGIPS Events in Cisco CTD

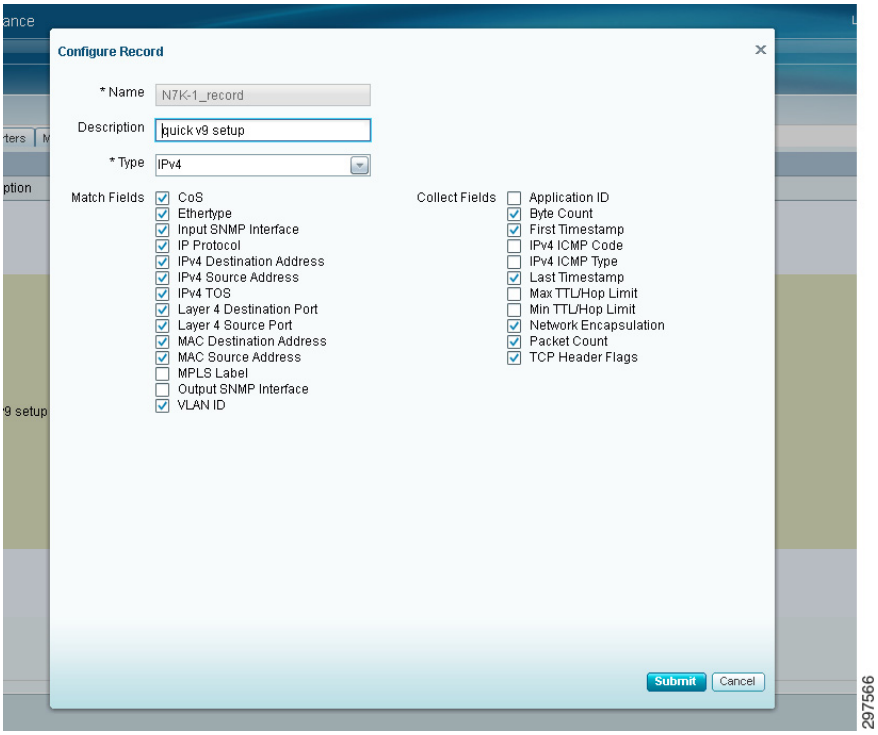


Integrating Generated NetFlow Records from Nexus 7000 Switches into Cisco CTD

High traffic rates for Nexus 7000 switches can result in the generation of NetFlow records that can put high loads on the switch CPU. To reduce Nexus 7000 CPU loads, NGA offloads the processing needed to generate NetFlow records. As shown in Figure 4-5, Nexus 7000 traffic is spanned to NGA, which converts raw traffic flows to NetFlow records. The records are then forwarded to the NetFlow collector in Cisco CTD.

As mentioned previously, NGA has four physical ports that receive data from various appliances. In this solution, two ports receive spanned data from the two Nexus 7000 aggregation switches. Optionally, the other two ports can receive data from the Nexus 5540 access switches. NGA can be configured to export a variety of NetFlow Version 9 record fields, as shown in Figure 4-5.

Figure 4-5 NetFlow Version 9 Record Fields Exported by NGA



Note Configure MAC-address fields only if managed device settings are configured. Refer to http://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_generation/1-0/user/guide/NetFlow_Generation_UG/getstarted.html#wp1134717 for details.

Integrating Generated NetFlow Records from ASA into Cisco CTD

As mentioned previously, unlike standard NetFlow, NSEL provides a stateful flow tracking mechanism that exports only those records that indicate significant events in an IP flow. NSEL events export data about flow status, and are triggered by the events that cause the state changes, rather than by activity timers as in standard NetFlow.

ASA (through NSEL) currently reports on the following event types:

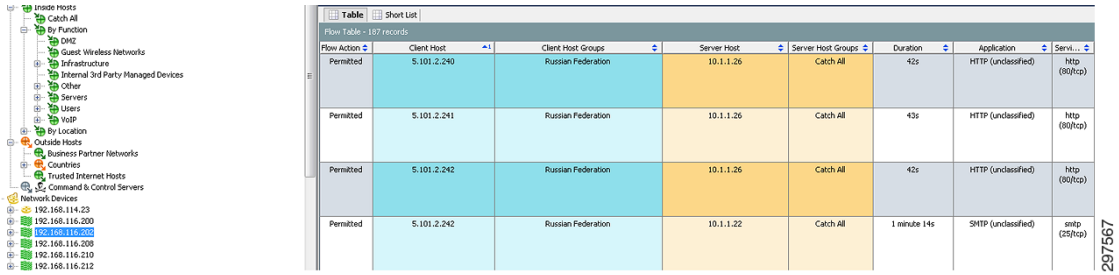
- Flow Create
- Flow Tear Down
- Flow Denied

The following highlights differences between NSEL and standard NetFlow:

- NSEL is bidirectional and sends one flow record per connection; other connections through Cisco IOS devices generate two flows per connection (one for each direction).
- NSEL report a total byte count for each bidirectional flow, rather than a byte count for each direction.
- NSEL does not report packet counts.
- NSEL has a predefined template for each reported event types; these templates are usually exported before any NSEL data records.
- NSEL flow-export actions are not supported in interface-based policies; flow-export actions can be applied only in a global service policy.

In NSEL records, information about reported events is transported in fields inside NSEL records. Cisco CTD's StealthWatch management dashboard interprets the fields and defines them as Flow Actions, as shown in Figure 4-6. If a flow is permitted through the firewall (indicated by flow-created and teardown events), the Flow Action field shows Permitted; if a flow is blocked by a firewall access control list (ACL), the Flow Action field shows Denied.

Figure 4-6 Viewing Flow Action Fields in Received NSEL Flows



The context provided by the Flow Action fields is considered by behavioral algorithms in StealthWatch, so the Flow Denied action can provide a useful inspection point to run queries and to identify suspicious activity, such as scanning and distributed denial of service (DDOS) attacks.

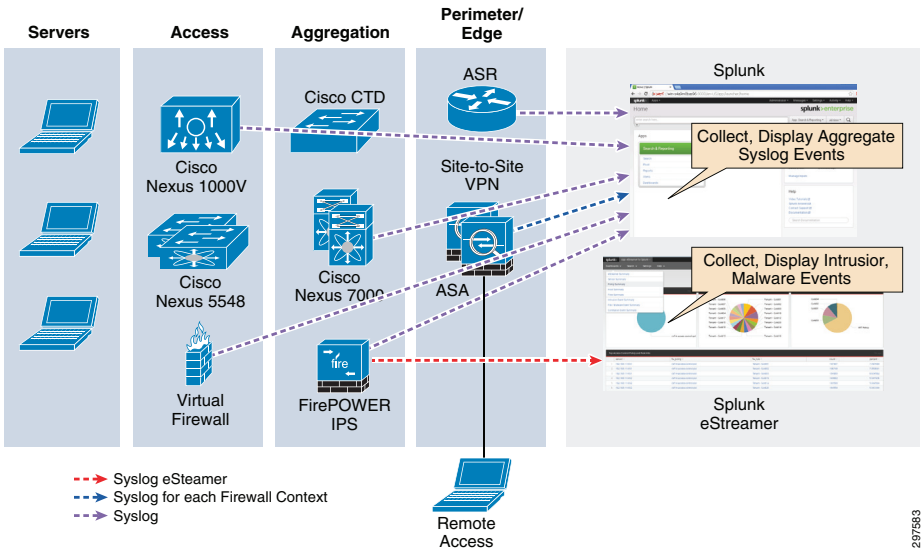
Tracking Events, and Threat Analysis using Splunk

From a security perspective Splunk supports a forensics approach to security event management. Looking for patterns in log data from Cisco and other security devices and viewing them in context of other data provides a comprehensive view of what's happening across an IT infrastructure. Using Splunk, the security team can harness their knowledge to model attack vectors and attack patterns based on conditions which Splunk can easily identify. As shown in this section, Splunk provides additional context to security events by connecting to external sources of data and pulling this data into generated reports or within a dashboard interface. Augmenting security data with information from other sources can help decrease response times.

Once a search across data sources is constructed, the user can save, run, and send the search results and graphical reports to others in PDF format on a scheduled basis or used to display results on a real-time dashboard. As shown below. network appliances and security devices export events and log information to Splunk.

Figure 4-7 shows the aggregation of network and security events using Splunk.

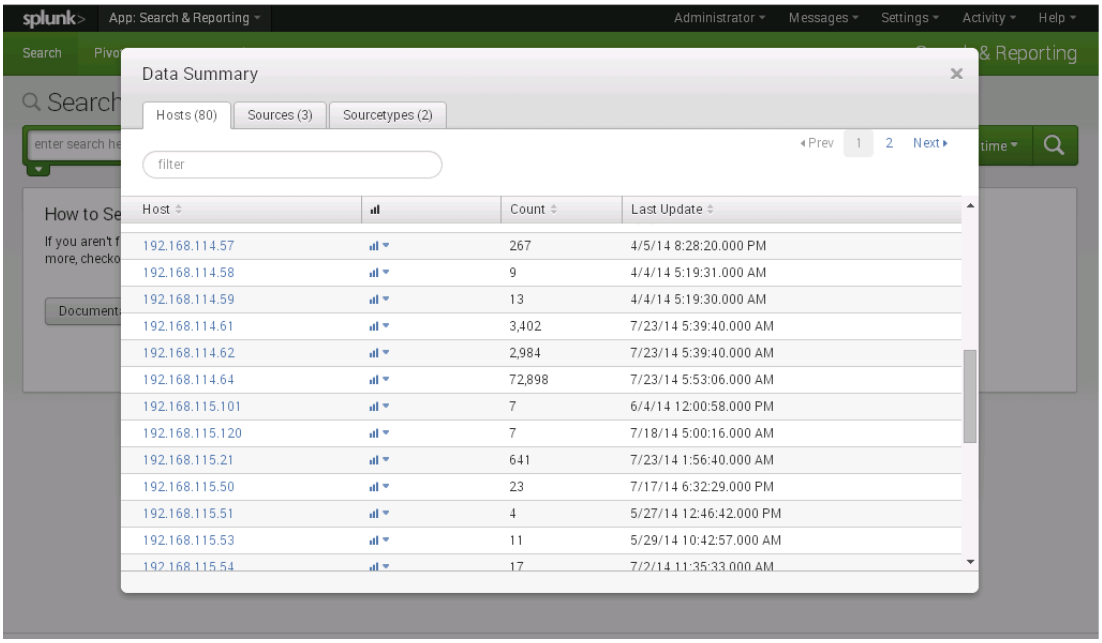
Figure 4-7 Splunk within VMDC



When deploying Splunk, note that:

- Each ASA context should be configured as a Syslog exporter. This enables ASA event tracking on a per-tenant basis.
- Cisco CTD can be configured to export Syslog records to Splunk and other appliances, such as FirePOWER.
- FirePOWER can be configured to send Syslog messages for intrusion events, malware events, and correlation events. Connection events can also be sent to Syslog servers on a per-tenant basis.
- Splunk can aggregate security and syslog events from network devices, including Nexus7000 Series switches, Nexus 5000 Series switches, Nexus 1000V virtual switches, and ASA, to provide a unified view of events in the network as shown below in Figure 4-8.

Figure 4-8 Event Aggregation in Splunk

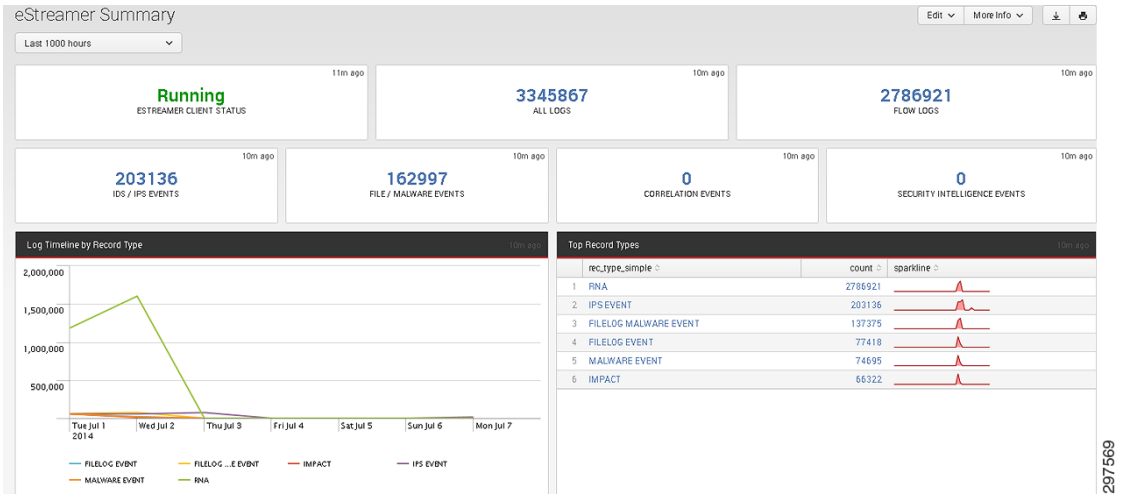


Tracking Events using eStreamer

The eStreamer Splunk is a community* created application that can track intrusion events, file and malware events, flow logs, correlation, and security intelligence events, in a real-time dashboard, from FirePOWER appliances, as shown in Figure 4-9.

Note Estreamer is a community created tool that is leveraged in this solution. It is not an officially supported application by Cisco Systems, for more information on installation and the application itself refer to https://support.FirePOWER.com/downloads/1533/fetch. and http://apps.splunk.com/app/1629/.

Figure 4-9 eStreamer Event Tracking



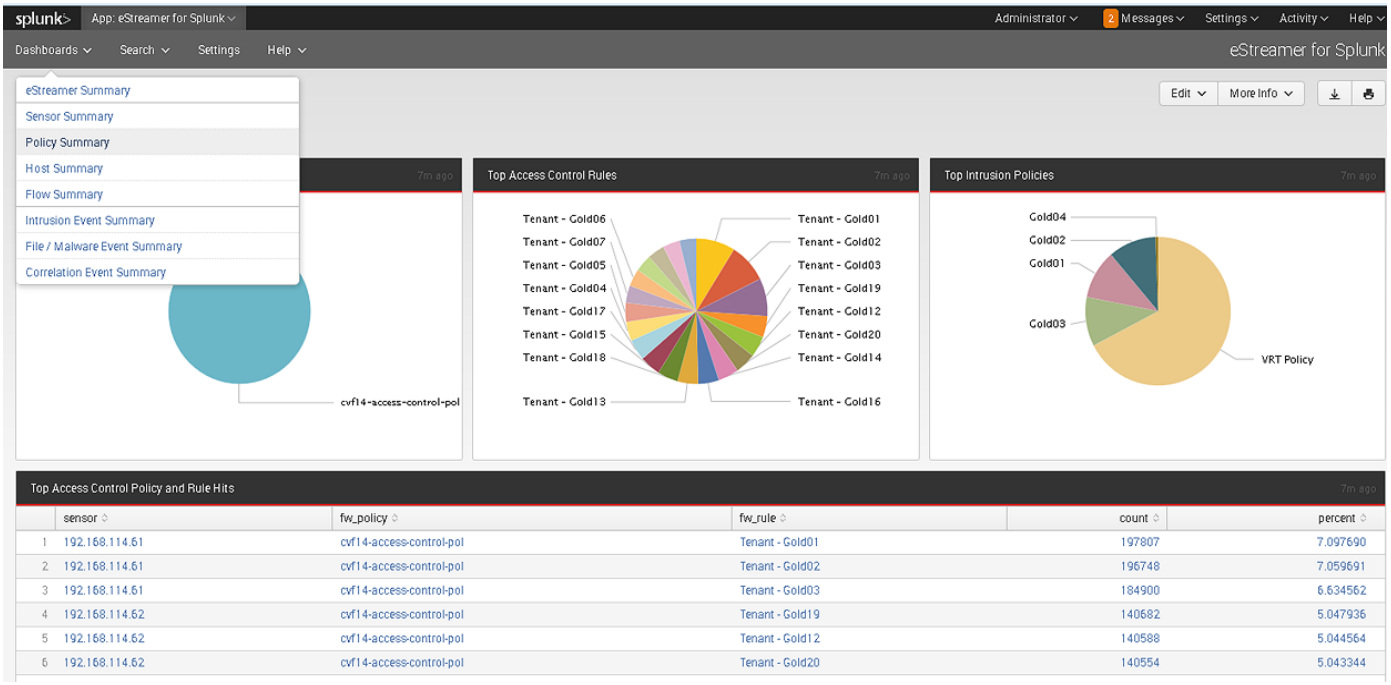
When deploying eStreamer, note that:

- A separate Splunk instance must be deployed to host an eStreamer application. In this solution, the FireSIGHT Management ConsolBotnetorwards event information to eStreamer application.
- It is possible to forward events directly from IPS appliances to eStreamer application. This requires deploying additional Splunk instances for each appliance.
- FirePOWER can be configured to forward Intrusion and Malware events to eStreamer and other events to another Splunk instance that is used for central log management.

The eStreamer dashboard enables security personnel to zoom in to particular Syslog message categories after possible anomalies or attacks are identified and obtain highly detailed event information from the logs. For example, as shown in Figure 4-10, you can zoom in to a policy summary in the dashboard and get a visual indication of policy-change events for different tenants over time. For example a spike in policy change events can indicate unauthorized access and tampering within the FirePOWER policy configuration.

Figure 4-10 displays access control policy and intrusion policy changes in the FirePOWER policy engine.

Figure 4-10 Aggregating policy events from FirePOWER using eStreamer Application



Event Correlation and Data Analysis

This section describes methods and a framework to correlate and prevent attacks using security components in the Virtualized Multiservice Data Center (VMDC) Cloud Security solution.

Note Full descriptions of them feature-rich solution components are beyond the scope of this document.

FirePOWER network security appliances and Cisco Cyber Threat Defense (CTD) provide complementary functions that can assist in effective event correlation and attack prevention. Table 4-2 and Table 4-3 compare the FirePOWER network security appliances and Cisco CTD.

Table 4-2 Solution Area Comparison

Solution Area	Sourcetire FireSIGHT	Lancope StealthWatch
Enterprise wide flow collections and storage	No	Yes
Build and maintain network Map providing real time context for intrusion event correlation	Yes	No
Large scale retrospective analysis on network traffic	No	Yes
Identification of suspicious activity through behavioral analysis	No	Yes

Table 4-3 Functional Comparison

Functionality	Sourcetire FireSIGHT	Lancope StealthWatch
Out of the box NBA	Manual	Yes
Application aware	Yes	Yes (with DPI Sensor)
Snort Rules	Yes	No
Packet retention	Yes	No
Leverage Netflow, sFlow IPFIX, AppFlow, and so on	Limited (NetFlow v5)	Yes
Flow retention	Weeks	Months or more
Host Map	Yes	No (Needs definition)
Traffic Profile signatures	Manual, limited	Yes
Post event flow analysis	Limited	Yes and longer term

Detecting Botnets

Botnets comprise distributed software that collectively performs malicious actions as dictated by a master server that controls the botnet. Botnets are installed on numerous computers using infected emails, web downloads, and Trojan horses. A botnet consist of two components: one or more infected bots and one or more botnet controllers.

A bot is a host that was compromised using a software tool kit that enables remote hacker control over useful host resources. A botnet server is software that collects information from the bots under its control. Botnet servers use the computing power of the bots under its control to carry out malicious acts, such as distributed denial of service (DDOS) attacks, sending spam, and stealing sensitive data.

A botnet server periodically communicates with the infected bots through a unidirectional data flow-from bots to server. Usually, the server passively collects information from the bots without responding, and waits for an opportune moment to simultaneously activate the bots.

The VMDC Cloud Security 1.0 solution uses the following methods to detect botnets.

Detecting Botnets Using FirePOWER Security Intelligence Events

FirePOWER can automatically detect botnets using its cloud-lookup security intelligence capabilities. To blacklist botnet servers, FirePOWER compares originating flow IP addresses with a list of known botnet servers. Figure 4-11 shows a list of blocked bot connections viewed under Connections > Security Intelligence Events.

Figure 4-11 Detected Botnets in FirePOWER Security Intelligence Events

Cisco CTD Beacon Host Detection

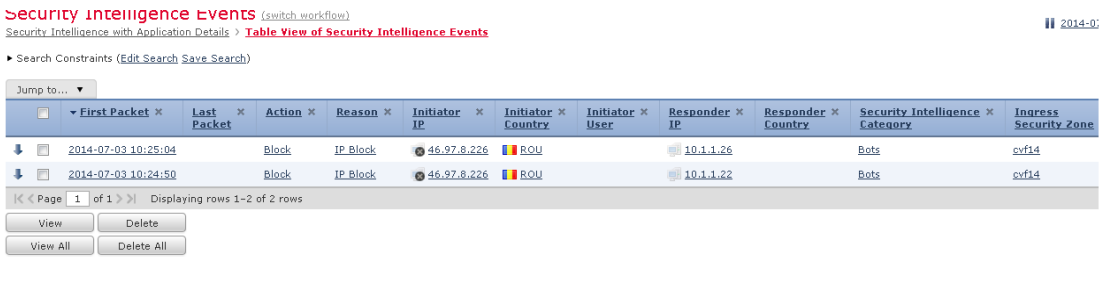
In general, botnets communicate from “inside” to “outside.” A beaconing host has an inside-to-outside communication flow that exceeds certain parameters, such a connection time. Cisco CTD generates an alert when it detects suspicious communication channels of that may be botnets.

By default, Cisco CTD trigger alarms when it detects beaconing hosts and changes the display coloring of the host from green to orange in the internal host-group navigation tree.

After a FirePOWER appliance or the Cisco CTD detects a botnet, it is imperative to determine whether additional internal hosts are infected. The target host IP address can be determined from FirePOWER connection events (shown in Figure 4-11), or by viewing the host IP address in the Cisco CTD botnet pane under the Cyber Detection Dashboard. Determining other possible infected host can be done by viewing the flow-table on the Cisco CTD of the host.

In addition the connection table within FirePOWER can be leveraged to see what other hosts the command center has tried to communicate with. Figure 4-12 shows a botnet server trying to communicate with two internal hosts.

Figure 4-12 Host Activities View

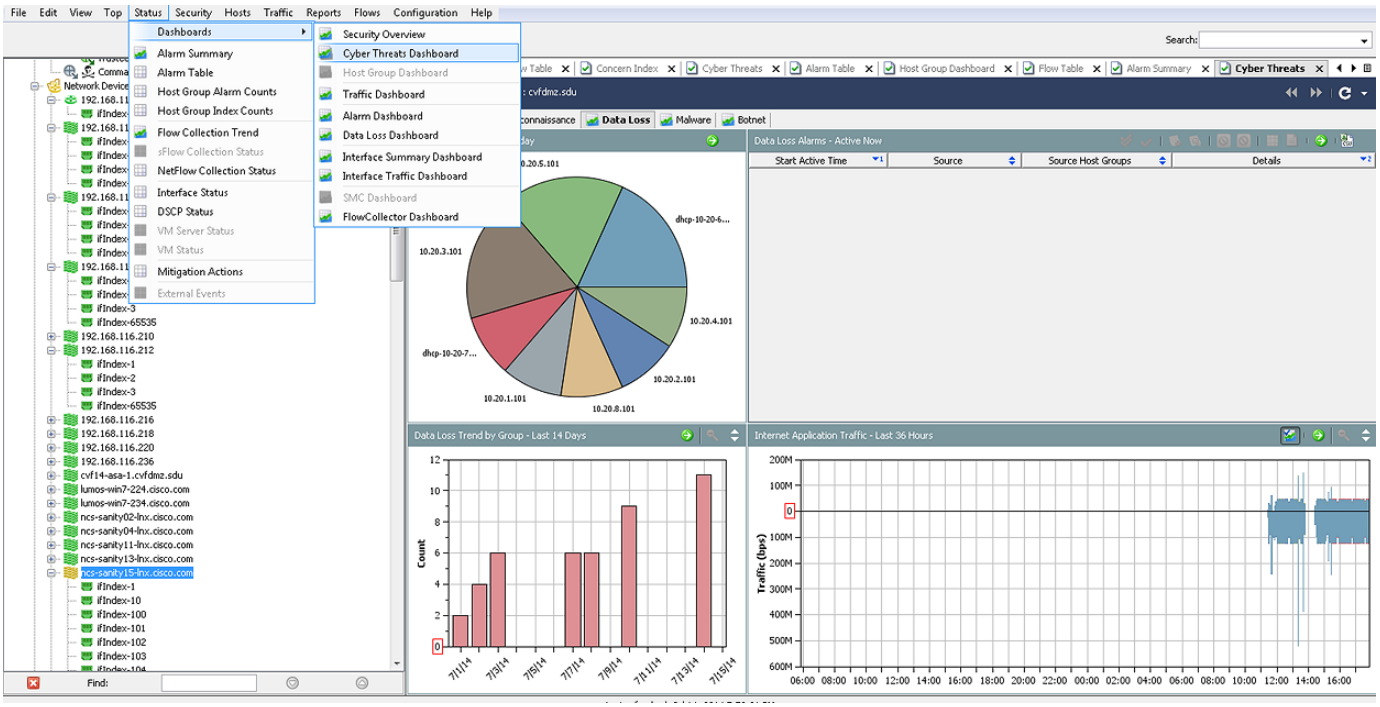


Detecting Data Loss

Data loss describes the loss of critical business data to unauthorized users. Data loss typically involves a data breach and back end transmission of sensitive data such as credit-card data, patient or financial information. Detecting data loss is imperative for implementing security controls for various compliance regimes such as PCI DSS and HIPAA. However, data loss incidents are unintentionally undetectable.

Data loss incidents normally involve asymmetrical outbound flows, in which outbound flows significantly outweigh a few inbound packets. Cisco CTD can trigger data loss alarms on such conditions. NetFlow generated flows contain flow direction, so Cisco CTD can leverage NetFlow generated flows and trigger data loss alarms on asymmetrical flows. Data loss events can be viewed using the data loss pane of the Cyber Threats Dashboard, as shown in Figure 4-13.

Figure 4-13 Detected Data Loss



To effectively detect data loss traffic flows, Cisco CTD captures and analyzes historical data about network flows, and uses the data to create a baseline for the network. Baselining can be performed on host groups, which are often defined by IP address ranges and can have descriptions such as Tenant-x-Servers. Cisco CTD creates behavior profiles of all hosts and tracks several for flows to the hosts many days. Cisco CTD continually monitors flows and compares them to baseline parameters to determine whether data loss event has occurred.

For more information about configuring Cisco CTD to detect data loss, refer to http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/threat-defense/detecting_data_loss_with_cyber.pdf.

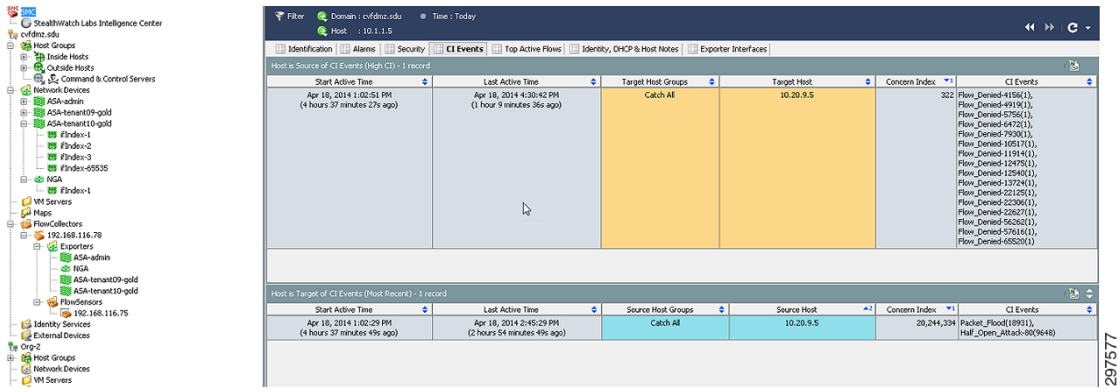
After a host is identified as a suspect in a data loss event, the connection table in FirePOWER or the flow table in Cisco CTD can provide more information about the receiving node or other potential suspects in the internal hosts.

Detecting DDOS Attacks Using NSEL and Cisco CTD

NSEL uses stateful records and indicates which host initiates a flow, it is easy to distinguish clients and servers. This characteristic makes NSEL an effective tool for detecting DDOS attacks.

ASA generates NSEL records for significant flow events (flow created, flow denied, and flow tear down). This information is sent to Cisco CTD in fields in the NSEL record. Cisco CTD's StealthWatch management dashboard interprets the fields and defines them in a flow action field. StealthWatch then uses the flow action field context in its behavior algorithm to generate a concern index (CI) for each flow. During DDOS attacks, high CI values are generated along with an alarm indicating an attack. As shown in Figure 4-14, one can use the CI Dashboard in StealthWatch to characterize the incoming attack for a given host.

Figure 4-14 Monitoring High CI Events to Detect DDOS Attacks



Because the byte count reported by NSEL represents data moving in both directions, it is difficult to separate how much data was uploaded or downloaded. Additionally, NSEL does not report packet counts, may hinder efforts to detect DDOS attacks using only NSEL data. Because NGA can intercepts north-south traffic, NGA exports traditional NetFlow to Cisco CTD for the same flows as NSEL. NGA can provide the missing timeout, packet, and byte data to complement ASA. This ensures complete flow visibility while maintaining unique context advantages delivered by NSEL.

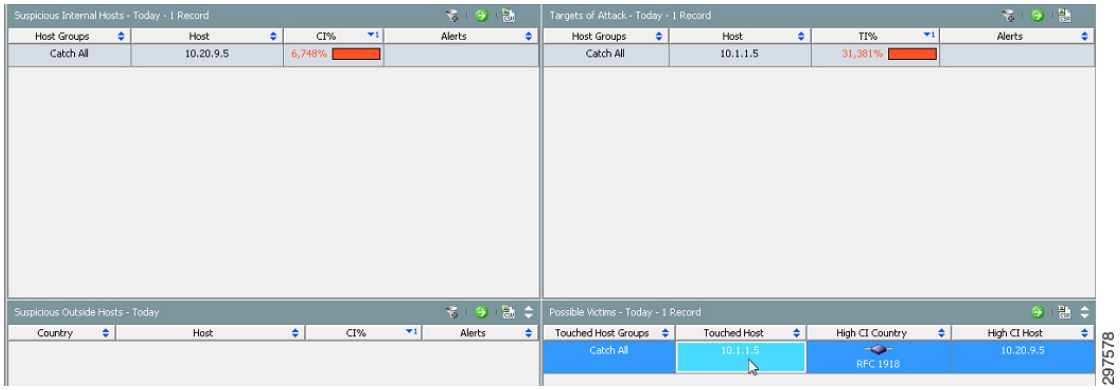
Detecting Reconnaissance Activities Using NSEL and Cisco CTD

The presence of network reconnaissance is one of the earliest indicators of an impending attack. The ability to detect reconnaissance early in the threat lifecycle is a critical part of a strong of a security framework. However, detecting reconnaissance inside the network perimeter is particularly challenging.

As in DDOS attacks, StealthWatch combines NSEL and NetFlow records from NGA to detect reconnaissance activities. For example, a device performing reconnaissance typically generates a large number of Address Resolution Protocol (ARP) requests but receives few responses. Other reconnaissance attacks generate illegal flag conditions such as SYN/FIN. In most cases, Cisco CTD can recognize these patterns to complement threat detection by appliances such as FirePOWER.

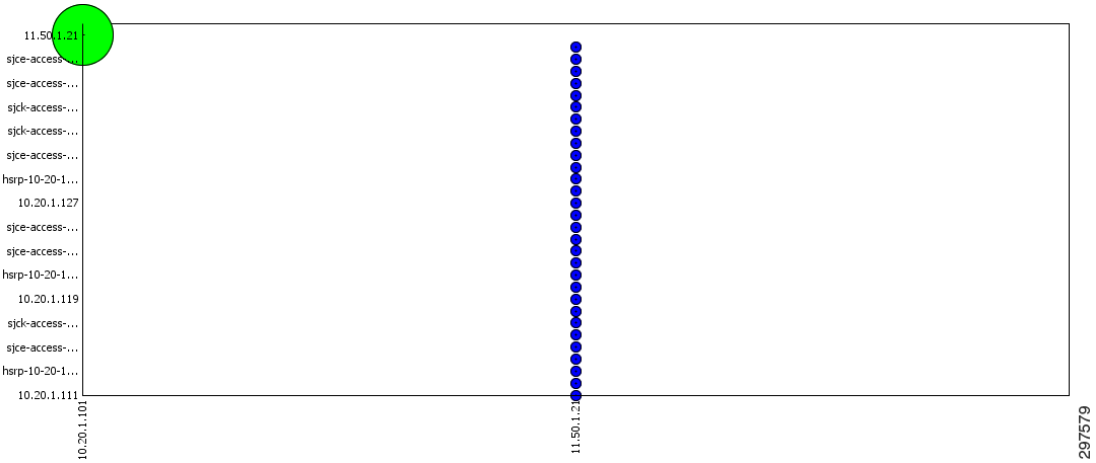
Cisco CTD's StealthWatch generates an alarm for high CI for a given host, providing an indication of scanning as shown in Figure 4-15.

Figure 4-15 Internal Host Scanning Indication



After determining the suspicious flow, by viewing the top active host for that flow, one may discern a high variance of destination IP addresses that uses "strange ports." In addition, by viewing the "Peer vs. Peer" and "Peer vs Port" views in the flow table display, one can view host activities during a specified time period. The "Peer vs Peer" view generates a table that maps internal hosts to IP addresses they communicated with, and "Peer vs Port" view generates a table, mapping the nodes and the ports they communicated with. Hosts that communicate with a wide range of receivers or a wide range of ports can be considered suspicious, as shown in Figure 4-16.

Figure 4-16 Peer-to-Peer View Scanning Indication



CHAPTER 5

Compliance

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in regulatory actions, including federal fines, and the possibility of litigation.

There are different regulatory compliance laws for different market verticals, such as the following:

- For credit card data, the PCI DSS is a regulation that organizations who process such information must adhere to
- For the health care segment, the HIPAA is a requirement
- Federal agencies and their service providers must adhere to the FISMA

Regulatory compliance not only creates a defense against the threat, but it also offers an opportunity to consistently strengthen your organization through strategic, proactive measures-such as best practices, employee training, internal technical and process controls.

Virtualization is a significant movement within IT environments that enables many organizations to reduce storage and processing costs while simplifying overall management and improving scalability. It does provide the improvement and efficiency of their workloads but on the other side it has a dependency on the hardware platform it is built on and the security of that hardware in terms of access and control. There are many degrees of virtualization, but all create a virtual representation of an operating system, server, storage device, or network resource in order to abstract operations from physical devices.

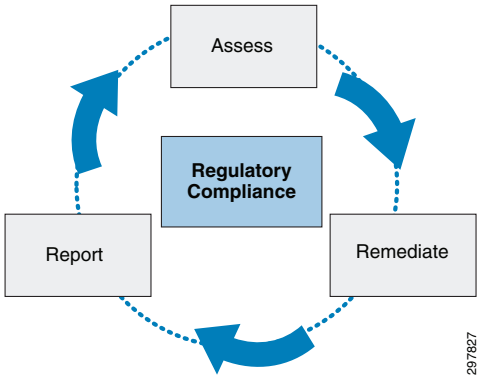
Virtualization has generated a trend toward cloud computing environments in which data, applications, and software based network overlay infrastructure can reside anywhere and services are delivered where needed, as needed, on demand to any device or end user.

Public clouds enable organizations to reduce their capitalized IT infrastructure, as well as management costs and complexity, by storing assets on a shared, but secured, hosted infrastructure. Enterprises can also build their own private clouds, with data center environments that can deliver cloud-based services within their own organization.

As there are benefits of public cloud and virtualization world, there are unique challenges, including but not limited to segmentation, data storage, access control, forensic auditing, logging, monitoring and alerting across complete network paradigm.

Compliance is not a one-time process, rather it is a continuous cycle of assessing the environment, re-mediating the issues, and then reporting and filing it.

Figure 5-1 Compliance Process Cycle



Although achieving compliance requires more than just technology, the network is critical in supporting organizations' compliance strategies. Cisco VMDC Cloud Security 1.0 offers a Unified Compliance Solution Framework with guidelines that facilitate addressing multiple regulatory compliance requirements from one network infrastructure. When working with the network, it is essential to address the scope of the compliance. The cost of compliance and complexity increases in proportion to the scope. Certain techniques and guidelines are provided on how to minimize the scope of the compliance more effectively and efficiently. There are some common themes among various compliance objectives, such as segmentation of traffic among tenants, identity and access control, and encryption of data at rest and in motion.

For example, it is recommended to use secure HTTP (HTTPS) and secure shell (SSH) Protocol that are secure replacements for the HTTP and Telnet protocols. The replacement protocols use secure sockets layer (SSL) and transport layer security (TLS) to provide device authentication and data encryption. These protocols are encrypted for privacy, and the unsecured protocols—Telnet and HTTP—are turned off on all the devices within the reference architecture.

In general there is a cost associated with achieving compliance that should be balanced against a potentially much larger set of costs if the organization is non-compliant.

Compliance Cost

Providing regulatory compliance on a cloud deployment infrastructure requires a larger initial investment for service providers. The following list shows a few areas where compliance can increase costs.

1. Technologies
2. Audits (Internal & External)
3. Remediation
4. Training
5. Management
6. Implementation

Other areas that can increase cost include proper processes, physical security, policies and planning.

Cost of Non-Compliance

As stated above, there are various factors that incur cost for achieving compliance as well as factors that incur much higher cost for non-compliance. Some of the key factors are shown below:

1. Significant Fines and Fees
2. Reputation of the service provider

3. Loss of production
4. Revenue Impact
5. Customer Relationship
6. Litigation or Arbitration Settlement Costs

To help reduce the risk of non-compliance, VMDC Cloud Security facilitates a service provider to achieve compliance for their cloud deployment in a more efficient manner by providing guidance and gap analysis in all three vertical deployments.

PCI DSS 3.0 Compliance Guidance

The PCI Data Security Standard (PCI DSS) provides guidance for securing payment card data. It includes a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents.

PCI Version 3.0 introduces new changes to the standard. The core 12 security areas as shown below are remain the same, but the updates include several new sub-requirements that did not exist previously. PCI version 2.0 will remain active until December 31st 2014 and organizations are required to comply with PCI, and PCI DSS version 3.0 officially goes into full effect on January 1, 2015 (Table 5-1).

Table 5-1 Service Provider Goals and PCI DSS Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

The PCI 3.0 new requirements are:

1. Lack of education and awareness
2. Weak passwords, authentication
3. Third-party security challenges
4. Slow self-detection, malware
5. Inconsistency in assessment

PCI DSS 3.0 changes are designed to help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice.

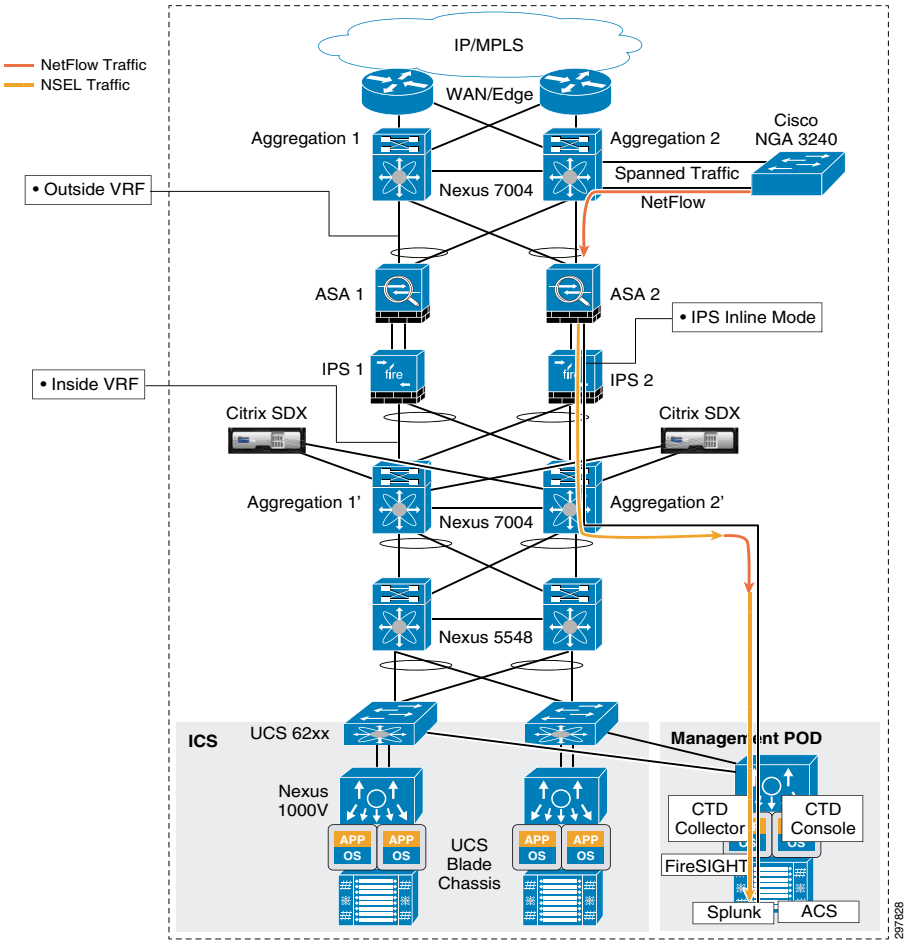
To overcome the challenge to meet these requirements, the VMDC Cloud Security 1.0 architecture includes next generation IPS, centralized password and authentication service, intelligent monitoring and network visibility tools such as Splunk and Cisco CTD, as described in the detail design section earlier in this document.

When service provider delivers cloud-based services to organizations such as financial institutions or organizations that store, process, or transmit cardholder data, those consumers are required to be compliant with PCI. However, not all organizations are required to meet the same number of controls. Control requirements are based on annual volume of credit card transactions, and the manner in which these credit cards are processed, transmitted, and/or stored. In some cases, the organization has the ability to self-assess for PCI Compliance. Organizations that process over six million transactions per year must have an annual assessment completed by a Security Assessor (independent third party or internal resource which has been approved by the PCI Security Standards Council).

In a multi services and multi-tenant cloud data center deployment model, the intelligent centralized log management is a key element for attaining PCI compliance. Cisco collaborated with technology partner Splunk to gather and aggregate logs from various components of the network and provide real time security event analysis and history of log management that can assist in a forensic investigation.

One of the greatest challenges to maintaining compliance the scope of the data center environment because if the service provider maintain their entire data center environment, it may not meet the PCI scope standards. A large scope may have devices and components that do not need to comply, but once in the scope, the PCI standards require these devices to be evaluated and audited. Figure 5-2 shows the layout of a complete data center network scope.

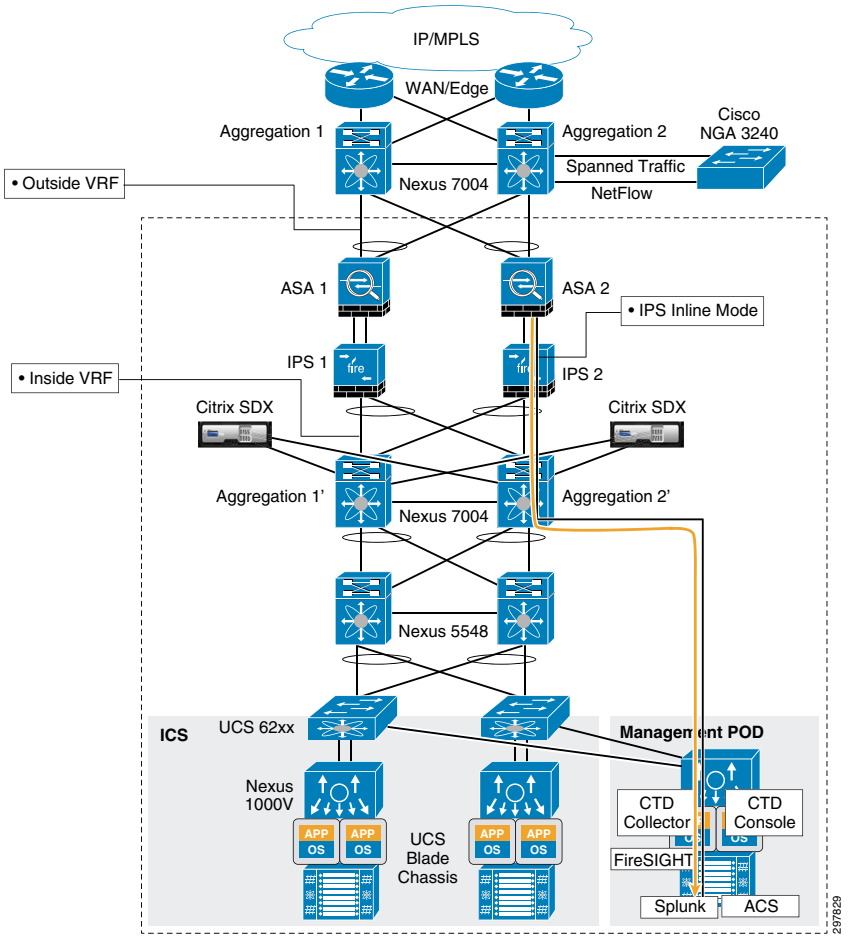
Figure 5-2 Scope of a Complete Data Center Network



As shown above, a service provider can bring in the 3rd party auditors to audit the entire data center including the NGA (Netflow generator appliance), WAN edge PE, and North VRF of Nexus 7K. This increases the scope of the PCI audit to include components outside the compliance scope. When scoping out network components within a data center, understanding the network and information flow is the primary step before properly selecting components.

In the network diagram above, there are various locations from where the security data has been collected, such as NetFlow traffic from Nexus 7K aggregation using NGA, and NSEL traffic from ASA, to the logging and monitoring device Splunk. The data collected from N7K and ASA are redundant in nature, due to the fact that all the customer traffic goes through the ASA firewall and thus, NetFlow traffic can be eliminated from the PCI scope, as shown in Figure 5-3.

Figure 5-3 Traffic Flow Through the ASA Firewall



In VMDC cloud security architecture, we have narrowed the scope to a limited section of the data center and eliminate the components that may not be required for PCI compliance.

Limiting the scope of the data center from a PCI perspective, as shown above, provides the ability for the VMDC cloud security architecture to achieve compliance efficiently.

PCI DSS 3.0 technical Control Mapping to VMDC Cloud Security 1.0 reference architecture is provided in Table 5-2.

Note This mapping is done based on the external audit with reference to the 12 major PCI DSS 3.0 requirements mentioned earlier.

Table 5-2 Mapping PCI DSS 3.0 to VMDC Cloud Security Reference Architecture

PCI DSS 3.0 Requirements	Total Controls	Controls Assist by VMDC	Controls Directly Achieved by VMDC	Product
Requirement 1	37	23	14	ACS, ASA, Splunk, BMC,
Requirement 2	30	13	0	Splunk, IPS, BMC
Requirement 3	44	Not Applicable	Not Applicable	Not Applicable

Table 5-2 Mapping PCI DSS 3.0 to VMDC Cloud Security Reference Architecture (continued)

PCI DSS 3.0 Requirements	Total Controls	Controls Assist by VMDC	Controls Directly Achieved by VMDC	Product
Requirement 4	11	Not Applicable	Not Applicable	Not Applicable
Requirement 5	11	Not Applicable	Not Applicable	Not Applicable
Requirement 6	44	3	1	IPS, VMDC Release Process
Requirement 7	10	9	0	ACS
Requirement 8	43	32	2	ACS, ASA
Requirement 9	45	Not Applicable	Not Applicable	Not Applicable
Requirement 10	41	35	3	Splunk, NTP server, N7K, N5K, ASA
Requirement 11	32	5	5	IPS, Splunk
Requirement 12	47	Not Applicable	Not Applicable	Not Applicable
Total	**395**	**120**	**25**	

For further details, refer to the Cisco Design Zone VMDC landing page.

Note The completion of a PCI DSS 3.0 assessment or guidance alone will not prevent a compromise of data. This information only addresses the capability of compliance for VMDC Cloud Security 1.0 reference architecture against PCI DSS 3.0 security requirements as published. Recommendations within this guidance are intended only to aid in compliance against the assessed control baselines and prioritized based on perceived business requirements.

HIPAA Compliance Guidance

VMDC Cloud Security 1.0 reference architecture provides guidance and tactical designs for HIPAA compliance. It clarifies how the data center network components can address requirements when a service provider delivers services to health professional or health related enterprises.

The HIPAA Omnibus Final Rule, released in January 2013, included updates from the Health Information Technology for Economic and Clinical Health (HITECH) Act, breach notification, penalty tiers, and extended HIPAA compliance obligations to include both covered entities and business associates. Any transaction that includes reception, transmission, storage or processing of protected health information (PHI) in electronic format need to comply with the HIPAA standards.

The VMDC Cloud Security 1.0 reference architecture uses the National Institute of Standards and Technology (NIST) publication 800-66, revision #1 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. NIST 800-66 encompasses requirements for Healthcare organizations and their downstream partners to ensure security and privacy of electronic Protected Health Information (ePHI).

Note NIST 800-66 control set applies solely within the United States in the form of the Health Insurance Portability and Accountability Act (HIPAA). While HIPAA is a United States statute, VMDC Cloud Security 1.0 reference architecture is versatile and supports configurations to meet stringent security and privacy requirements as they apply to International or Non-United States based entities.

The service provider - when deploying the data center for providing services to healthcare enterprises - may be required to meet certain administrative, physical and technical safeguards as described by the US Department of Health and Human Services.

The HIPAA Omnibus Final Rule consists of three main sections:

- **Part 160**—General Administrative Requirements. Deals mostly with the legal, compliance, and penalty aspects of HIPAA.
- **Part 162**—Administrative Requirements. Deals with unique identifiers for covered entities in healthcare, provisions for transactions, and many other administrative issues in healthcare.
- **Part 164**—Security and Privacy. Deals with the safeguards for protecting PHI in electronic and paper media. Part 164 consists of the following:
  - **Subpart A**—General Provisions §164.1xx
  - **Subpart B**—Reserved
  - **Subpart C**—Security Standards for the Protection of Electronic Protected Health Information §164.3xx
  - **Subpart D**—Notification in Case of Breach of Unsecured Protected Health Information §164.4xx
  - **Subpart E**—Privacy of Individually Identifiable Health Information §164.5xx

Note From infrastructure perspective, the VMDC Cloud Security 1.0 reference architecture is primarily focused on Part 164 subpart C (§164.3xx).

The VMDC Cloud Security 1.0 reference architecture does not guarantee HIPPA compliance; rather it facilitates and provides guidance for achieving compliance. The responsibility for compliance is always on the data owner.

Table 5-3 shows the mapping of the HIPAA rule controls to VMDC components. It should be noted that there are many controls under each section. For example, under 164.312 rule, there are more than 20 controls.

For details about the complete list of controls, service provider needs to review the HIPAA compliance standards.

Table 5-3 HIPAA Control Mapping to VMDC Cloud Security Reference Architecture

HIPAA RULE	VMDC Facilitate	VMDC Directly Support	Product
164.310(b)	Yes		N7K, N5K, ASA, IPS, FI, UCS, ACS, NGA, Cisco CTD, Splunk Storage, Server Blades
164.310(d)(1)	Yes		Server Blades, ESXi, VMware
164.312(a)(1)		Yes	ACS
164.312(a)(2)(i)		Yes	ACS
§164.312(a)(2)(ii)		Yes	ACS, Splunk
§164.312(b)		Yes	Splunk
§164.312(c)(1)		Yes	ACS
§164.312(c)(2)		Yes	Splunk, IPS
45 CFR § 164.304		Yes	ACS

Table 5-3 HIPAA Control Mapping to VMDC Cloud Security Reference Architecture (continued)

HIPAA RULE	VMDC Facilitate	VMDC Directly Support	Product
§164.312(d)		Yes	ACS
§164.312(e)(1)		Yes	ASA, SSL VPN
§164.312(e)(2)(i)		Yes	ASA, VPN
§164.312(e)(1)(ii)		Yes	ASA, VPN

There are four major categories that reduce the risk of losing control over PHI data:

- Segmentation, page 5-9
- Identity and Access Management, page 5-9
- Logging, Auditing, and Monitoring, page 5-10
- Encryption and Decryption, page 5-10

Segmentation

Segmentation is a basic building block when becoming HIPAA compliant. In a multi-tenant cloud deployment model, the service provider needs to ensure all tenants are completely segmented into their individual containers. In some cases within an enterprise, segmentation and isolation is required from HIPAA perspective, especially if one department is dealing with PHI data and others are not. The VMDC Cloud Security 1.0 reference architecture built the segmentation and isolation of each tenant end-to-end, using techniques like Layer 3 VRF, Layer 2 VLAN, separate firewall context, VSAN and intra-tenant segmentation VSG. This segmentation using switches may apply to the HIPAA Safeguard for guarding against malicious software as described in 164.308(a)(5)(ii)(B).

The need to segment, separate, and isolate administrative and PHI data is huge in limiting the scope and depth of security controls that are applied for HIPAA compliance. By segmenting PHI data from administrative information, service providers can protect PHI data by applying the appropriate controls. Proper segmentation and QoS play a key role in terms of hosting a health care provider. Huge files, such as imaging, xrays, can be transferred across a server safely and rapidly.

Firewalls also play a key role in segmenting the traffic and protecting PHI data. The Access Control Lists (ACLs) provide explicitly permitted and/or denied IP traffic that may traverse between inside, outside, and DMZ zones. Routing and access control lists provide segmentation between authorized and unauthorized access on the network. This capability can be mapped to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i).

Identity and Access Management

VMDC Cloud Security 1.0 reference architecture recommends the centralized identity and access management using Cisco ACS server. Cisco Secure Access Control System (ACS) is a highly scalable, policy-based network access and device access administration control platform that centralizes:

- Network device administration control
- Flexible and granular user authentication and authorization control
- Controls network and device access based on dynamic conditions and attributes

- Access to multiple Identity Databases, both internal and external such as Active Directory

Identity management, authentication, authorization, and access control of users and systems to PHI is the central theme in the HIPAA Security Rule safeguards. A strong and manageable identity and access control solution is critical for achieving an assessment finding of a low level of risk under a risk management program in HIPAA.

As mentioned above, Identity Management should be centralized from the compliance perspective, however in case of failure of the centralized system, compliance requirements may specify that local identity and access management be configured for emergency access. For example, if an ACS server went down and a health professional needed to access a certain critical application, the service provider administrator should be able to provide some emergency access. This ensures that the ability to control system access during both routine and emergency events is supported. The HIPAA security rule 164.312.(a)(1) Access Control requires that technical policies and procedures be implemented to allow access only to authorized persons or software programs. All non-authorized personnel should not have access even during the potential failure of the centralized authorization service.

Logging, Auditing, and Monitoring

A particularly critical requirement of the HIPAA Security Rule is the logging, auditing, intrusion detection and monitoring of PHI data within the service provider environment. In this reference architecture, Splunk plays a key role as a centralized component for collecting application, database, device and user access logging as well as the enablement of auditing that is critical to effectively supporting a service provider or business associates breach management strategy. For HIPAA compliance, real time intrusion detection and protection of all the tenants that generate PHI or ePHI data is paramount, especially in a large and complex data center deployment such as the VMDC Cloud Security 1.0 reference architecture, where such intrusions and malware may become breaches if not detected in a timely fashion. To provide such services, the reference architecture uses NextGen IPS that detects and applies deep packet analysis and inspection at line rate. It performs the following:

- Access global intelligence with the proper context to make informed decisions and take immediate action.
- Consistently enforce policies across the entire network and have the control to accelerate threat detection and response.
- Detect, understand and halt advanced malware/advanced persistent threats across the entire attack continuum.

For example, the IPS/IDS identify, protect or block individuals or data that post suspicious activity within the data center. This falls under the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).

Logging, auditing, and monitoring are critical factors for a service provider to meet HIPAA Accounting Rule 164.528, and can help identify whether a compromise has occurred that may lead to a breach notification.

As mentioned above, the logging should be centralized, but to meet compliance in case of centralized system failure, the logging should be enabled on each of the HIPAA scoped components locally.

Encryption and Decryption

According to the HIPAA Security Rule, the PHI data must be kept secure during transmission under the addressable implementation specification for encryption. There should be application layer encryption, but additional consideration should be given when PHI leaves the health related enterprise, such as

clinics over Internet service provider (VPN). For example, in this reference design, the recommendation is to have SSL VPN between end customers and the service provider cloud data center where the services are deployed. To protect the PHI data and prevent unnecessary exposure, encryption and decryption plays a most effective role. This enables service providers to meet the HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption. Providing encryption of traffic over public networks meets the HIPAA requirement for Transmission Security 164.312(e)(1), Integrity 164.312(e)(2)(i), and Encryption 164.312(e)(2)(ii).

Typically, when healthcare-related tenants transmit PHI data over the Internet to the centralized data center, is the data is secured as a demilitarized zone (known as DMZ). In this reference architecture, firewall and IPS are used to provide a DMZ zone for all Internet access from any healthcare related tenants.

Details on how to create DMZ zone within the VMDC Cloud Security 1.0 reference architecture can be found using the link below:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-3/design_guide/VMDC_2-3_DG.pdf

Note The completion of a HIPAA assessment or guidance alone will not prevent a compromise of data. This information addresses only the capability of compliance for VMDC Cloud Security 1.0 reference architecture against HIPAA security requirements as addressed by NIST. Recommendations within this guidance are intended only to aid in compliance against the assessed control baselines and prioritized based on perceived business requirements.

FISMA Compliance Guidance

Title III of the E-Government Act, also known as FISMA, requires federal agencies or their service providers to implement risk-based information security programs. The National Institute of Standards and Technology (NIST) provides the Risk Management Framework in a series of Federal Information Processing Standards (FIPS) and special publications.

To meet compliance requirements of the Federal Information Security Management Act (FISMA), service providers and federal agencies must include planning, processes, and technology together to make effective use of resources and money while protecting the confidentiality, integrity, and accessibility of mission-critical information systems.

To aid in both cost-effectiveness and risk-based decision making, information systems are categorized based on the type of information being processed. The resulting categorization is then utilized to select the appropriate security controls to be implemented. Once implemented, the controls are assessed and if appropriately applied, are authorized for operation within the federal sector. Continuous monitoring activities take place to ensure security controls continue to operate and provide sufficient protection.

Without a thorough understanding of FISMA and security control implementations, many solutions do not integrate FISMA compliance into their development life cycles. Without security integration, configuring solutions to comply with FISMA becomes a complicated and tedious process contributing to excessive financial and labor costs. Organizations will find implementing new solutions into an existing architecture is similar to fitting a square peg into a round hole for each individual control. In some instances, system customization must be performed to meet requirements. These complications add onto an existing high-dollar compliance program.

The Self-Defending Network is Cisco's strategy to protect federal organizations from security threats caused by both internal and external sources. This protection enables government agencies and their service providers to take better advantage of the intelligence in network resources, thus improving overall security while addressing FISMA requirements.

The VMDC Cloud Security 1.0 solution can facilitate service providers to meet FISMA requirements, including mitigations for unauthorized access, malicious code, scans and probes, improper usage, and denial-of-service attacks.

Challenges and Guidance

In an increasingly dynamic environment facing advanced persistent threats, the challenge of effectively achieving and maintaining FISMA compliance can be significant. Within a data center, virtualization is another key challenge that can delay and jeopardize compliance if not properly deployed with various security controls.

The biggest challenge with FISMA is that most organizations do not have personnel that fully understand the FISMA compliance process. The NIST recommended controls are very non-prescriptive and thus are not easily understood by typical IT staff. This means that the already time consuming task of working towards FISMA compliance becomes almost impossible with inexperienced staff.

Another challenge is that there are no “out of the box/off the shelf” solutions to ensure compliance with specific technical controls. Most hardware and software put into place have to be meticulously configured in a way that is not covered in the manufacturer’s guide to meet the control requirements. Configuring the hardware and software considered in scope for FISMA compliance requires extra time to research, test, and implement these changes, all while still being unsure whether or not it’s actually meeting the requirement.

The FISMA Gap Assessment process focused on the security of information systems by determining whether Cisco has effectively implemented the capabilities required to apply adequate security measures that comply with the requirements as outlined by NIST.

VMDC Cloud Security 1.0 reference architecture was assessed against a moderate impact baseline. 86 of 265 controls were applicable, including controls within Access Control, Audit and Accountability, Identification and Authentication, System and Services Acquisition, System and Communication Protection, and System and Information Integrity families.

Implementation

The VMDC Cloud Security 1.0 reference architecture assessment found all 86 of the controls identified above as being satisfied when an organization implements the Cisco VMDC architecture in accordance with Cisco's configuration documentation. These controls aid service providers by providing guidance with numerous NIST control families including Access Control, Audit and Accountability, Identification and Authentication, System and Services Acquisition, System and Communication Protection, and System and Information Integrity. Leveraging the technical controls defined by and audited within the Cisco VMDC architecture provides better guidance for service providers who need to meet the FISMA requirements.

Integration of the VMDC solution into a FISMA compliant architecture will allow service providers, large enterprises, and federal agencies to mitigate impacts on two levels: system integration, and system management. Service providers deploying VMDC 2.x-based reference architecture are capable of implementing predefined configurations that are known to be compliant, and more importantly, secure, using Cisco best practices and recommendations.

During the FISMA audit, auditors subject the VMDC solution to a rigorous assessment that resulted in 86 security controls for direct implementation. The second level of impact exists where organizations have the capability of integrating the VMDC solution into a secure environment and adapting existing operational and management controls. This two-tiered benefit achieves FISMA alignment for secure system integration and management within the environment.

The VMDC Validated Design feature 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 NextGen IPS provides deep packet inspection and blocks all possible cyber threats before they can impact the network. Similarly the network visibility tools and log monitoring help service providers to see the full picture of their network continually to better enable proactive management in a timely fashion. All of these security features within VMDC provide a seamless mapping and integration of FISMA controls.

Considerations

The Federal Information Security Management Act (FISMA) framework establishes baseline security criteria for all Federal Agencies and contractors for the United States Government. Currently the standard is on Revision 4 and applies solely within the United States. Applicable only within the United States, many common requirements are shared by International Standards. The reference architecture is a versatile solution and supports configurations to meet stringent security and privacy requirements as they apply to international or non-United States based entities.

FISMA Compliance & VMDC Cloud Security Reference Architecture Mapping

There are various areas that FISMA requires to be addressed before any organization attempts to attain FISMA compliance. A summary of the VMDC solution's ability to meet such compliance requirements are shown in the table below. There are controls from various sections of FISMA guidance that may not apply to directly to VMDC. For example: training and awareness for information security personnel, maintenance, and physical protection for the network and data center.

With all the complexity surrounding FISMA, organizations can find the compliance process challenging. VMDC alleviates obstacles by taking care of the majority of the most difficult technical requirements to implement. By using VMDC, organizations can focus their efforts on the operational and management controls associated with FISMA, allowing them to move quickly through the compliance process.

Several tools are available within the VMDC environment to help facilitate FISMA compliance; including ASA firewalls, Cisco FirePOWER IDS/IPS, Lancope StealthWatch, Cisco ACS, and Splunk.

Customized ASA firewalls are used to properly segment each organization's FISMA boundary from other environments. Firewalls are required between any FISMA and non-FISMA environment per the System and Communication Protection family of FISMA controls.

Splunk, which is Security Information and Event Management (SIEM) software, covers many of the FISMA controls within the environment, including the Audit and Accountability family of controls. Audit and Accountability requires the use of a centralized log server that has the ability to discover and alert upon anomalies within the logs.

The Cisco FirePOWER Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) monitor both inbound and outbound network traffic. If anomalies are found throughout the monitoring process, Cisco FirePOWER can be configured to email an organizational resource an alert when it has identified malicious traffic. For specific types of anomalies, the IPS function of the appliance will automatically

identify attack signatures and prevent the malicious traffic from occurring in the future. This layer of security helps cover requirements across all areas, but mainly assists in the implementation of controls within the System and Communication Protection family of FISMA controls.

Cisco CTD uses network device telemetry to provide deep, complete visibility across the network core, enabling security operators to understand and use network traffic details to discover anomalies. Deploying Cisco CTD across networks can provide information and visibility to support security operators in a variety of threat detection tasks, including:

- Data loss detection
- Network reconnaissance of internal networks
- Monitoring the spread of malware in internal networks
- Botnet command and control channel detection in internal networks

Implementation of Cisco CTD assists in meeting FISMA requirements mainly from Audit and Accounting and Incident Reporting that include forensic audit capability.

Cisco Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that operates as a centralized RADIUS and TACACS+ server. It extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user-productivity gains.

Cisco Secure ACS enforces a uniform security policy for all users regardless of how they access the network. It reduces the administrative and management burden involved in scaling user and administrator access to the network. By using a central database for all user accounts, Cisco Secure ACS centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network.

Cisco Secure ACS provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. It helps to ensure enforcement of assigned policies by allowing network administrators to control:

- Who can log into the network
- The privileges each user has
- Security audit or account billing information
- Access and command controls for each configuration's administrator

Cisco Secure ACS addresses concerns about compliance by supporting features associated with administrator permission and audit reports:

- Administrative constraints on log settings restrict administrators from disabling certain types of logging.
- Forced administrator password change at login prompts administrators to change the password at configurable time intervals.
- Administrator password policy provides a mechanism to enforce a configurable minimum password length and mix of characters (upper/lower case, numeric, punctuation).
- Forced administrator password change for stale account enforces password change when the administrator has not logged on in for a specified number of days.
- Generation of entitlement reports provides a report that shows all administrator privileges.
- Password history for administrators prevents reuse of passwords.

ACS helps service provider to meet FISMA requirements in multiple areas such as Access control, Audit and Accounting, Risk Management and Identification and Authentication.

Table 5-4 FISMA Control Mapping to VMDC Cloud Security Reference Architecture

Compliance Section Number	Section Title	Total Controls	Controls Facilitated by VMDC	Product Mapping
AC	Access Control	35	19	ACS, IPS, Nexus Switches, ASA, Cisco CTD, SPlunk
AT	Awareness and Training	5	0	Not Applicable
AU	Audit and Accounting	17	10	ACS, Splunk, Cisco CTD, IPS
CA	Security Assessment and Authorization	10	2	ASA, IPS, Splunk
CM	Configuration Management	19	7	ASA, IPS, BMC management tool
CP	Contingency Planning	23	4	MDS, NetApp
IA	Identification and Authentication	22	13	ACS, ASA, All products with password complexity
IR	Incident Response	12	2	Splunk, Cisco CTD, IPS
MA	Maintenance	10	0	Not Applicable
MP	Media Protection	9	1	NetApp
PE	Physical and Environment Protection	20	0	Not Applicable
PL	Planning	6	0	Not Applicable
PS	Personnel Security	8	1	Splunk
RA	Risk Assessment	7	1	ACS
SA	System and Services Acquisition	14	1	VMDC documentation
SC	Systems and Communication Protection	27	17	ACS, N7K, N5K, IPS, ASA, NetApp,
SI	System and Information Integrity	21	8	Splunk, IPS
Total		**265**	**86**	

For further details, refer to the Cisco Design Zone VMDC landing page.

Note The completion of a FISMA assessment or guidance alone does not prevent a compromise of data. This guide addresses only the capability of compliance for VMDC Cloud Security 1.0 reference architecture against FISMA security requirements as published by NIST. Recommendations within this guidance are intended only to aid in compliance against the assessed control baselines and prioritized based on perceived business requirements.

Benefit of VMDC Cloud Security Guidance towards FISMA Compliance

Specific benefits include:

1. **Demonstrated solutions to critical technology-related problems in evolving IT infrastructure—**Provides support for cloud computing, applications, desktop virtualization, consolidation and virtualization, and business continuity.
2. **Reduced time to deployment—**Provides best-practice recommendations based on a fully tested and validated architecture, facilitating technology adoption and rapid deployment.
3. **Reduced Risk—**Enables enterprises and service providers to deploy new architectures and technologies with confidence.
4. **Increased Flexibility—**Provides rapid, on-demand, workload deployment in a multi-tenant environment using a comprehensive automation framework with portal-based resource provisioning and management capabilities.
5. **Improved Operating Efficiency—**Integrates automation with a multi-tenant pool of computing, networking, and storage resources to improve asset use, reduce operation overhead, and mitigate operation configuration errors.