White Paper

Cisco Secure Enclaves Architecture

Design Guide

Contents

Introduction

This document discusses the reliable and transparent introduction of Cisco® Services in the data center to create a more flexible, functional, and secure application environment.

Goals of This Document

The purpose of this design document is to propose an IT security framework that conforms to established design principles and to provide details about solutions arising from this framework, called the Cisco Secure Enclaves architecture. This document considers both the design and the composition of components to develop a coherent security model that takes into account both the hardware and software at every level of a Cisco integrated infrastructure stack. The goal of the design is to provide appropriate security that provides desirable levels of performance and fault tolerance with ease of management at a competitive price.

Audience

This document is intended to provide technical direction to channel partners and end-user customers interested in making security an integral part of their IT infrastructure. The need for security is even greater when IT resources are shared among groups of people whose data cannot be shared. This design and future implementations arising from it address the challenges and requirements of such a shared platform.

Challenges and Objectives

Most computing platforms are designed to meet performance and function requirements with little or no attention to trustworthiness. Furthermore, the movement toward optimal use of IT resources through virtualization has resulted in an environment in which the true and implied security accorded by physical separation has essentially vanished. System consolidation efforts have also accelerated the movement toward co-hosting on integrated platforms, and the likelihood of compromise is increased in a highly shared environment. This situation presents a need for enhanced security and an opportunity to create a framework and platform that instills trust. Lack of confidence that such a trust environment can be delivered with ease and maintained with resilient resource management is a major obstacle to the physical consolidation of applications and adoption of cloud-computing service models.

The Cisco Secure Enclaves architecture helps evolve the current converged infrastructure offerings of Cisco by simplifying and standardizing the delivery of Cisco application and security services on architecturally consistent platforms. This approach is a logical extension of these data center building blocks, advancing the benefits of standardization beyond the infrastructure to the applications and services required. This design provides the following features that facilitate a uniform approach to IT in the data center:

- Flexible consumption model, allowing customer requirements to be met from both application and business perspectives
- Automation of well-known and well-understood resource pools of networking, computing, and storage resources
- Onboarding of services and applications
- Platform hardening and automation of security operations such as:
  - Configuration
  - Auditing
  - Patching
  - Responses
- Operation compliance and certifications

Design Overview

Infrastructure as a service (IaaS), from the provider perspective, consists of a set of modular building blocks of underlying resources assembled systematically based on services requested and overlaid with security. Services may be introduced either through dedicated appliances or through virtual appliance implementations on shared general-purpose computing resources. The main design objective is to help ensure that applications in this environment meet their subscribed service-level agreements (SLAs), including confidentiality requirements, by using pretested and validated IT infrastructure components to prevent inefficiency and inaccuracy.

Business Benefits

Many enterprises and IT service providers are developing cloud service offerings for public and private consumption. Regardless of whether the focus is on public or private cloud services, these efforts share several common objectives:

- Cost-effective use of capital IT resources through co-hosting
- Better service quality through virtualization features
- Increased operation efficiency and agility through automation

One essential characteristic of cloud architecture is the capability to pool resources, and each tenant that subscribes to computing, networking, and storage resources in a cloud is entitled to a given SLA. The power savings brought about by consolidation also contributes to reduced total cost of ownership (TCO). Achieving these goals can have a positive impact on profitability, productivity, and product quality. However, the use of shared infrastructure and resources in cloud services architecture introduces new challenges, hindering widespread adoption by IT service providers, who demand highly efficient management of securely isolated customer and application environments.

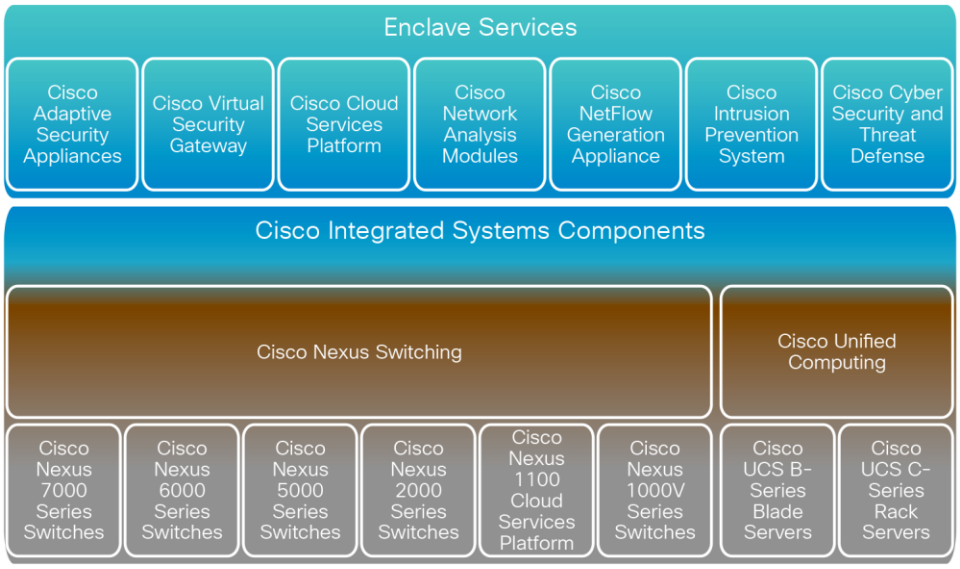
Enabling enterprises to migrate such environments to cloud architecture requires the capability to provide customer confidentiality while delivering the management and flexibility benefits of shared resources. Both private and public cloud providers must secure all customer data, communication, and application environments from unauthorized access. Such separation, with regulatory compliance measures, must be complete and consistent to instill confidence and achieve widespread adoption.

Architectural Overview

The Cisco Secure Enclaves design uses the common components of Cisco Integrated Systems along with additional services integration to address business and application requirements. These functional requirements promote uniqueness and innovation in the integrated computing stack that augment the original design to support these prerequisites. The result is a region, or enclave, and more likely multiple enclaves, in the integrated infrastructure designed and built to address the unique workload activities and business objectives of an organization.

The common foundation of the Cisco Secure Enclaves design is Cisco Integrated Systems. Cisco Integrated Systems combines the Cisco Unified Computing System™ (Cisco UCS®) and Cisco Nexus® platforms with technology from leading storage vendors. The result is a standardized infrastructure and the foundation to rapidly deliver data center applications, virtualized desktops, and cloud computing services. Figure 1 illustrates the Cisco structural elements currently used in Cisco Integrated Systems. The enclave infrastructure foundation is formed using a subset of these components.

Figure 1. Cisco Integrated Systems Components



Note: For more information about Cisco Integrated Systems, go to http://www.cisco.com/c/en/us/solutions/data-center-virtualization/integrated-systems/index.html.

The enclave strategy is a logical extension of the foundational platforms found in Cisco's converged infrastructure stacks. The enclave maintains the traditional design pillars associated with the shared computing stack architectures, which provide service assurance and enterprise-class availability in the data center. This foundation is readily extended to include organic and supplementary security services enabled or attached to this base as the application workloads or business initiatives require. Figure 2 shows a generic physical layout of Cisco Integrated Systems components that constitute the foundation of the enclave model.

Figure 2. Cisco Integrated Systems Physical Components

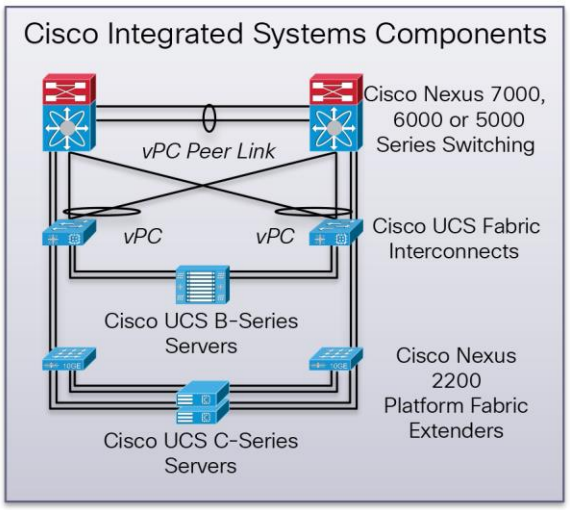
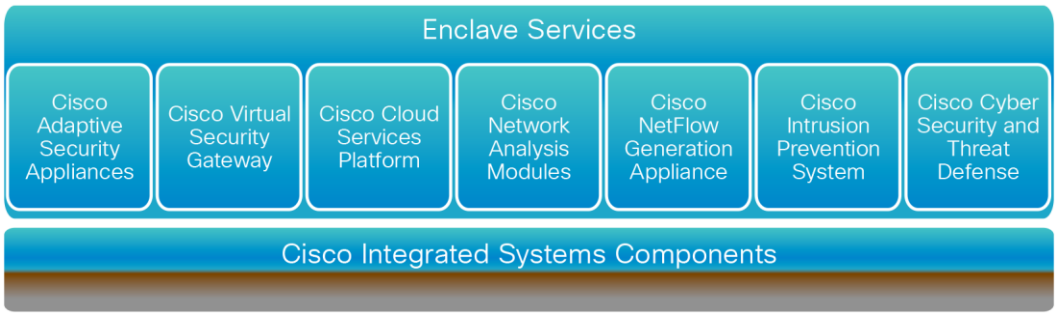


Figure 3 shows the extension of Cisco Integrated Systems to include features and functions beyond the foundational elements. Access controls, visibility, and threat defense are all elements that can be uniformly introduced into the system as required. The main feature of the enclave is the extensibility of the architecture to integrate current and future technologies within and upon its underpinnings, expanding the value of the infrastructure stack to address current and future application requirements.

Figure 3. Cisco Secure Enclaves Architecture Structure



The augmentation of the converged infrastructure stacks can be both physical and virtual. Figure 4 and Figure 5 illustrate the addition of physical Cisco Adaptive Security Appliances (ASA) Next-Generation Firewall Services. This platform offers services including Cisco Application Visibility and Control (AVC), Web Security Essentials (WSE), and Intrusion Prevention System (IPS).

Figure 4 shows a more traditional Cisco ASA high-availability pair deployment model in which the Cisco Nexus switches provide a connection point for the appliances. Cisco offers a number of Cisco ASA models to address the organization's specific scale requirements.

Figure 4. Physical Extension of Cisco Integrated Systems with Cisco ASA Security Services

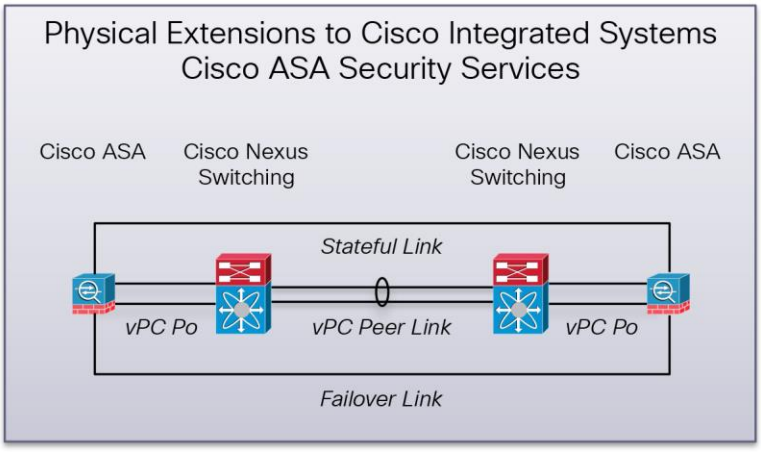
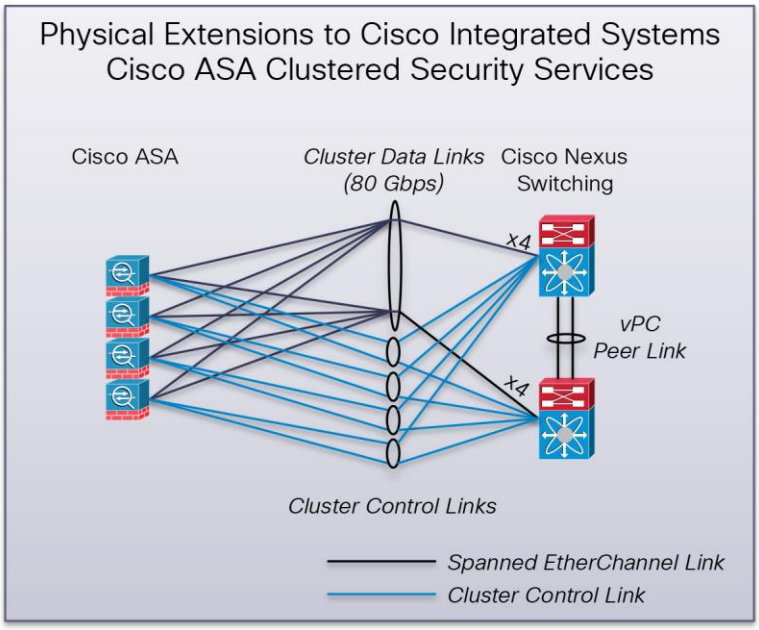


Figure 5 introduces the Cisco ASA platforms to a secure enclave as a clustered service. The Cisco ASA cluster model scales up to a maximum of eight nodes managed as a single unit. In clustered mode, every member of the cluster is capable of forwarding every traffic flow and can be active for all flows.

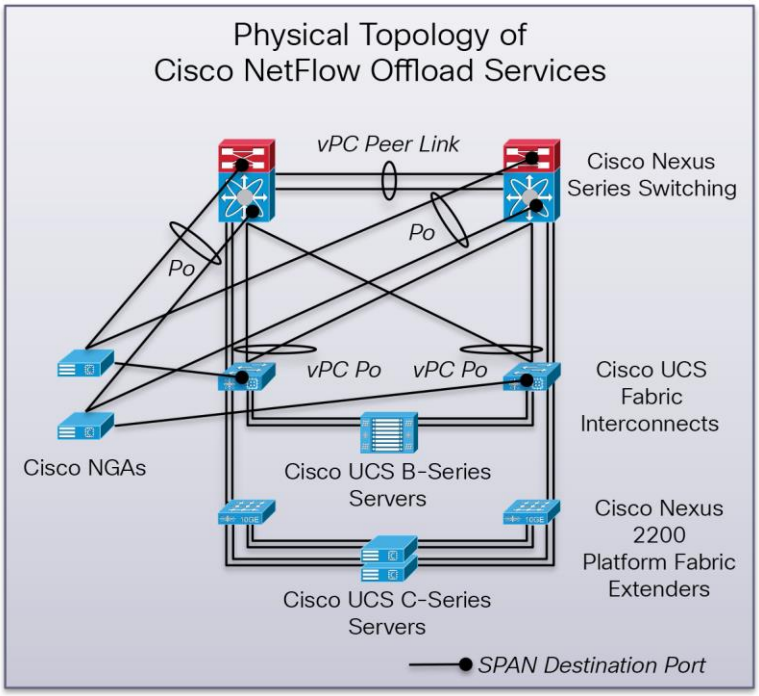
Note: Currently, Cisco ASA clustering is supported only for the Cisco Nexus 7000 Series switching platforms because of the need for Cisco Link Aggregation Control Protocol (LACP) support.

Figure 5. Physical Extensions of Cisco Integrated Systems with Cisco ASA Clustered Security Services



In addition to the Cisco ASA platforms, the integrated stack readily supports other services. For example, the Cisco NetFlow Generation Appliance (NGA) introduces a highly scalable, cost-effective architecture for cross-device flow generation. The Cisco NGA generates, unifies, and exports flow data, empowering network operations, engineering, and security teams to boost network operations excellence, enhance services delivery, implement accurate billing, and harden network security. Figure 6 shows the deployment of Cisco NGA on the stack to provide these services, accepting mirrored traffic from various sources of the converged infrastructure as Cisco NetFlow source data.

Figure 6. Physical Extensions of Cisco Integrated Systems with Cisco NetFlow Offload Services

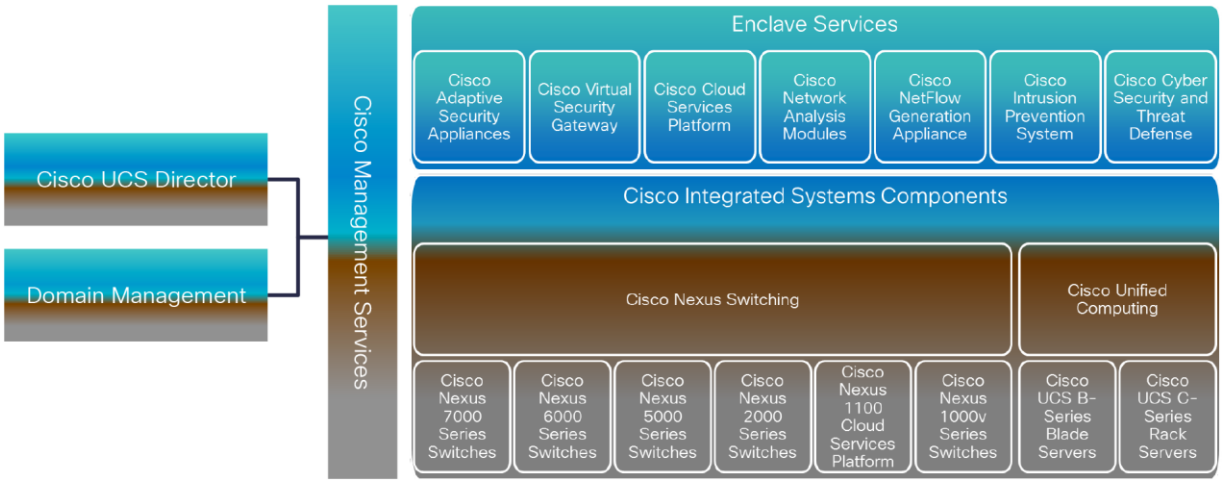


The strategic value of the enclave framework is the capability of the structure to adapt to an organization's needs. Supporting other physical appliance-based services beyond the Cisco ASA and NGA platforms is certainly feasible. "The Enclave" section of this document describes the blending of physical and virtual services to construct one or multiple unique regions.

The management of the enclave can be performed by individual domain managers or unified through Cisco UCS Director (Figure 7). Cisco UCS Director offers converged infrastructure management and extensions to control additions to the stack. Either model allows an organization to maintain traditional policy roles associated with computing, networking, and storage resources and security groups. The enclave framework currently uses the following domain management platforms:

- Cisco UCS Manager
- Cisco Prime™ Network Services Controller (NSC)
- Cisco Identity Services Engine (ISE)
- Cisco Security Manager
- Lancope StealthWatch Management Console

Figure 7. Cisco Secure Enclaves Management Structure



Security Philosophy: The Reference Monitor

The three most basic and necessary characteristics of the components that enforce security and instill trust are as follows:

- The mechanism must be protected from modification by unauthorized methods and users.
- The mechanism must not be allowed to be bypassed.
- The mechanism must be simple to understand and monitor.

These core requirements together help ensure the trustworthiness of the enforcement module: the Monitor.

Design Principles

Design principles are rules and guidelines instituted to help ensure, inform, and support the way in which an architectural implementation fulfills its mission. They provide a means to tie components and methods to the business objectives: protection, performance, and provisioning.

In a security platform, trust is paramount and must not be misplaced. In a system consisting of components of varying levels of trustworthiness, the assumption is that the overall trustworthiness of the system matches the least trustworthy subcomponent. Security is enforced through access control, which requires complete visibility into whatever is being secured. Relevant principles, the rationale for inclusion in an enclave, and the scope of an enclave are summarized here.

- **Least-common mechanism:** This principle states the need to globalize common and shared modules (in the enforcement domain). It has the effect of reducing duplicates, which can result in fewer opportunities for compromise. It also has the advantage of less overhead, because there are fewer instances, and potentially better performance. Another positive effect of implementing this principle is ease of maintenance.
- **Reduced sharing:** In the user domain, no computer resource should be shared between components or subjects unless it is necessary to do so. This approach helps prevent both inadvertent and deliberate encroachment. When information needs to be shared, it should be done only if sharing has been explicitly requested and granted.

- **Efficient mediated access:** As with most IT systems, development of secure systems includes interaction between hardware and software mechanisms. In a hierarchically constructed system with hardware constituting the lowest layer, when possible the most efficient choice is to allocate an access mediation mechanism to the hardware. Although hardware implementations provide greater performance, software equivalents provide flexibility, which is crucial in devising an adaptable solution. The principle of efficient mediated access strikes a balance between two possibilities by stating that access control functions should be allocated to the lowest possible level (closer to hardware) that still meets flexibility requirements.

These design principles, although they may appear contradictory, are complementary when their respective scopes are clearly defined. The first two principles are relevant in different spaces: the enforcement and user domains. Such principles are brought together to achieve a protected platform that can perform as desired and be provisioned with ease and correctness when required. Adopting global and dedicated appliances such as Cisco ASA firewalls and Cisco NGA devices enable desired levels of performance for the most critical elements (least-common mechanism) while also conforming to the reference monitor tenet of preserving the fidelity of the enforcement module. Management of Cisco ASA with Cisco Security Manager and authentication and authorization services provided by Cisco ISE software demonstrate the flexibility brought about by a centralized and global policy and configuration engine. User-domain abstractions are encapsulated in fenced containers (enclaves) automated through Cisco UCS Director, providing efficient mediated access.

After implementation, the platform needs to be able to continuously enforce data protection at every stage of the life of information, through encryption, to help ensure integrity. Techniques used to deploy the model components should be repeatable for easy and correct construction. The orchestration capabilities of Cisco UCS Director are used for this purpose. Eventually, every engineered system is a work in progress and so must take into account planned upgrades and maintenance. A system composed of simple and essential components contributes to reduced complexity and better understanding. Other criteria that facilitate easy adoption include less intrusive and more intuitive interfaces with clear user expectations of security risk.

The Enclave

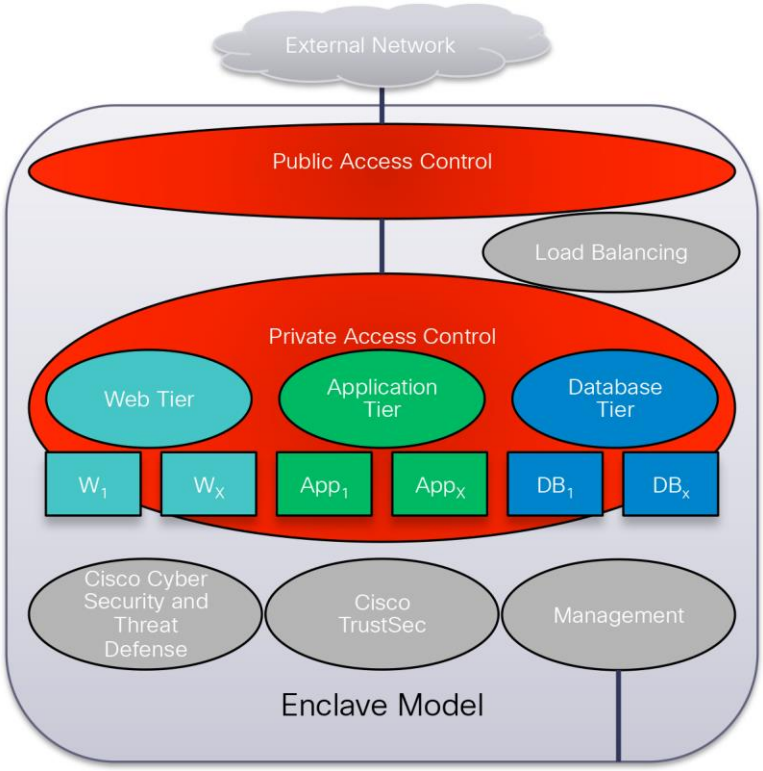
The enclave is a distinct logical entity that encompasses essential constructs including security along with application or customer-specific resources to deliver a trusted platform that meets SLAs. The modular construction and automated delivery help make the enclave a scalable and securely separated layer of abstraction of the design philosophy. The use of multiple enclaves delivers increased isolation, addressing disparate requirements of the converged infrastructure stack.

Figure 8 provides a conceptual view of the enclave that defines an enclave in relation to an n-tier application.

The enclave provides the following functions:

- Access control point for the secure region (public)
- Access control within and between application tiers (private)
- Cisco Cyber Security and Threat Defense operations to expose and identify malicious traffic
- Cisco TrustSec® security using secure group access control to identify server roles and enforce security policy
- Out-of-band management for centralized administration of the enclave and its resources
- Optional load-balancing capabilities

Figure 8. Cisco Secure Enclaves Model



The components that form the enclave may vary in form factor and be physical or virtual, and the requirements for functions may be based on business or application needs, but the structure is consistent in its form and manageability. The next sections discuss the enclave model to provide a better understanding of the system, its components, and their roles. The topics discussed include:

- Host topology
- Enclave topology
- Traffic patterns

Note: The Cisco Secure Enclaves architecture is hypervisor independent. The details provided here address a VMware vSphere deployment. Future efforts will address other virtualization platforms.

Host Topology

Standardizing the host topology through Cisco UCS service profiles improves IT efficiency. Figure 9 shows the uniform deployment of VMware ESXi within the enclave framework.

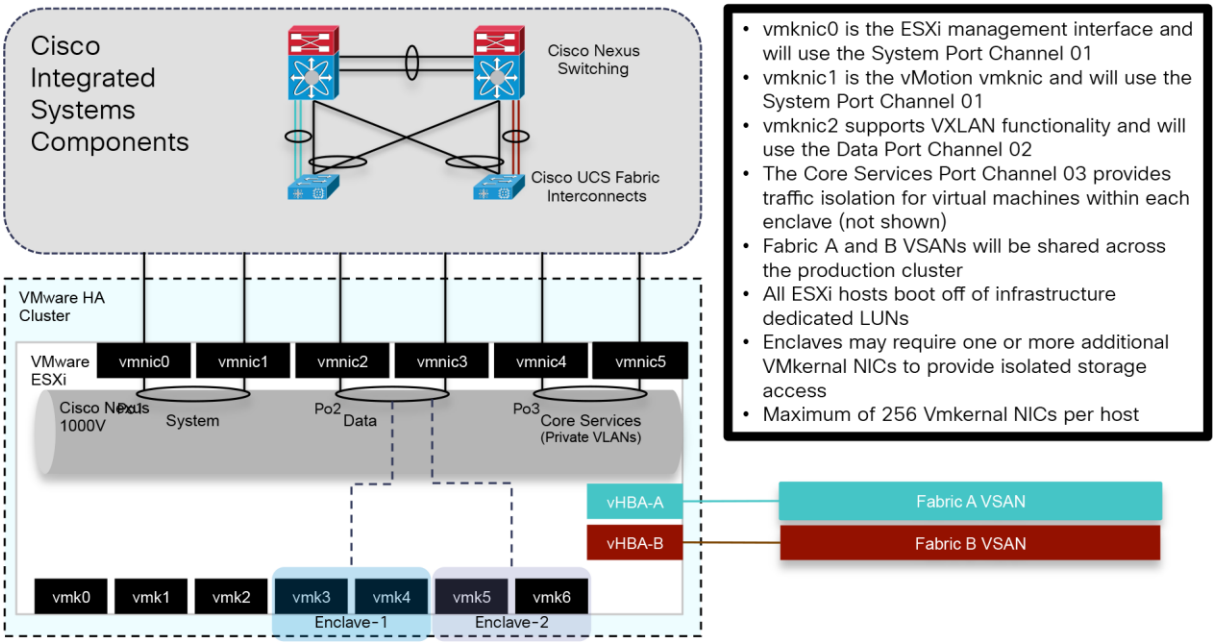
The main features include:

- The VMware ESXi host resides in a Cisco converged infrastructure.
- The VMware ESXi host is part of a larger VMware vSphere High Availability (HA) and Distributed Resource Scheduler (DRS) cluster
- Cisco virtual interface cards (VICs) offer multiple virtual PCI Express (PCIe) adapters for the VMware ESXi host for further traffic isolation and specialization.
  - Six Ethernet-based virtual network interface cards (vNICs) with specific roles associated with the enclave system, enclave data, and core services traffic are created:
    - vmnic0 and vmnic1 for the Cisco Nexus 1000V system uplink support management, VMware vMotion, and virtual service control traffic.
    - vmnic2 and vmnic3 support data traffic originating from the enclaves.
    - vmnic4 and vmnic5 carry core services traffic.
  - Private VLANs isolate traffic to the virtual machines within an enclave, providing core services such as Domain Name System (DNS), Microsoft Active Directory, Domain Host Configuration Protocol (DHCP), and Microsoft Windows updates.
  - Two virtual host bus adapters (vHBAs) for multihoming to available block-based storage.
- Four VMkernal ports are created to support the following traffic types:
  - vmknic0 supports VMware ESXi host management traffic.
  - vmknic1 supports VMware vMotion traffic.
  - Two VMknics (vmknic2 and vmknic3) provide the Virtual Extensible LAN (VXLAN) tunnel endpoint (VTEP) to support traffic with path load balancing through the Cisco UCS fabric.
- Additional Network File System (NFS) and Small Computer System Interface over IP (iSCSI) VMknics can be assigned to individual enclaves to support application and segmentation requirements. These VMknics use the PortChannel dedicated to enclave data.

Note: A maximum of 256 VMkernal NICs are available per VMware ESXi host.

- Cisco Nexus 1000V is deployed on the VMware ESXi host with the following elements:
  - PortChannels created for high availability and load balancing
  - Segmentation of traffic through dedicated vNICs, VLANs, and VXLANs

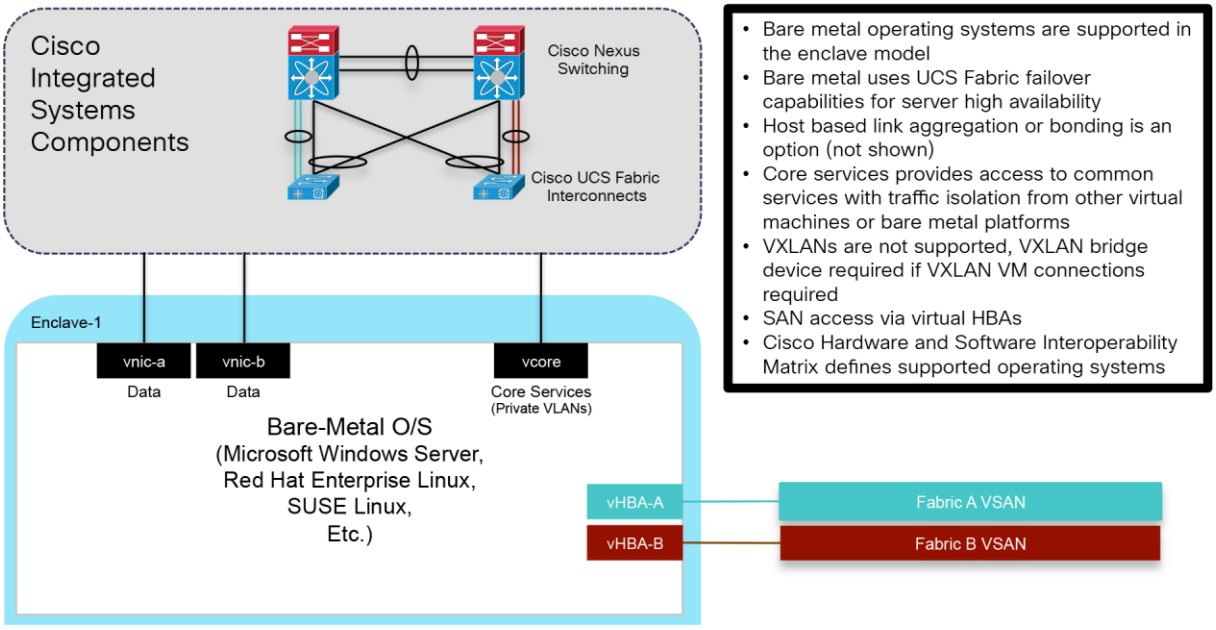
Figure 9. VMware ESXi Uniform Host Topology



The enclave architecture is not restricted to virtualized server platforms. Bare-metal servers persist in many organizations to address various performance and compliance requirements. To address bare-metal operating systems within an enclave (Figure 10), the following features were enabled:

- Cisco UCS fabric failover to provide fabric-based high availability
  - This feature precludes the use of host-based link aggregation or bonding.
- Cisco VICs to provide multiple virtual PCIe adapters to the host for further traffic isolation and specialization
  - Ethernet-based vNICs with specific roles associated with the enclave system, enclave data, and core services traffic are created:
    - vnic-a and vnic-b support data traffic originating from the host. Two vNICs were defined to allow host-based bonding. One vNIC is required.
    - vcore supports core services traffic.
  - Private VLANs isolate traffic to the virtual machines within an enclave, providing core services such as DNS, Microsoft Active Directory, DHCP, and Microsoft Windows Updates.
  - Two virtual HBAs provide multihoming to available block-based storage.
- Dedicated VLANs per enclave for bare-metal server connections

Figure 10. Bare-Metal Host Topology



Enclave Topology

The enclave can be broken down to its components, the combination of which creates the design and, ultimately, an efficient, consistent, and secure application platform. The instantiation of this design can be further standardized by using automation tools such as Cisco UCS Director as a delivery mechanism. This section describes two enclave models and their components and capabilities.

Figure 11 depicts an enclave using two VLANs, with one or more VXLANs used at the virtualization layer. The VXLAN solution provides logical isolation within the hypervisor and removes the scale limitations associated with VLANs. The enclave is constructed as follows:

- Two VLANs are consumed on the physical switch for the entire enclave.
- The Cisco Nexus 7000 Series Switch provides the policy enforcement point and default gateway (SVI 2001).
- Cisco ASA provides the security group firewall for traffic control enforcement.
- Cisco ASA provides virtual context bridging for two VLANs (VLANs 2001 to 3001 in the figure).
- VXLAN is supported across the infrastructure for virtual machine traffic.
- Consistent security policy is provided through universal security group tags (SGTs):
  - The import of the Cisco ISE protected access credential (PAC) file establishes a secure communication channel between Cisco ISE and the device.
  - Cisco ISE provides SGTs to Cisco ASA, and Cisco ASA defines security group access control lists (SGACLs).
  - Cisco ISE provides SGTs and downloadable SGACLs to the Cisco Nexus switch.
  - Cisco ISE provides authentication and authorization across the infrastructure.

- An SGT is assigned on the Cisco Nexus 1000V port profile.
- The Cisco Nexus 1000V propagates IP address–to–SGT mapping across the fabric through the SGT Exchange Protocol (SXP) for SGTs assigned to the enclave.
- The Cisco VSG for each enclave provides Layer 2 firewall functions.
- Load-balancing services are optional but readily integrated into the model.
- Dedicated VMknics are available to meet dedicated NFS and iSCSI access requirements.

Figure 11. Enclave Model: Transparent VLAN with VXLAN (Cisco ASA Transparent Mode)

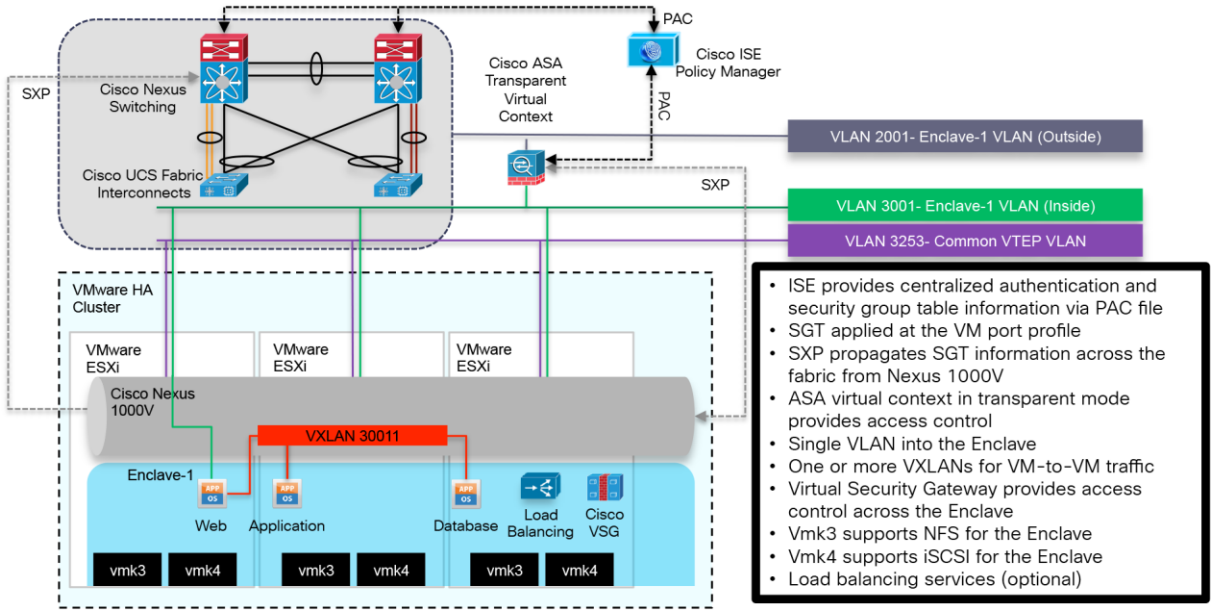
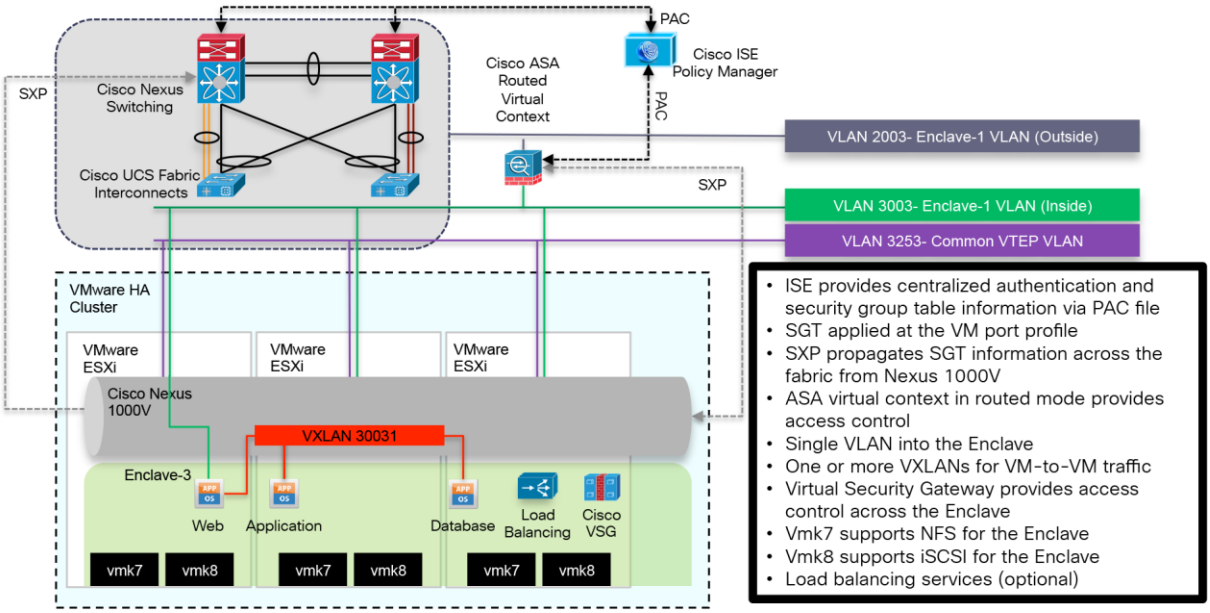


Figure 12 illustrates the logical structure of another enclave on the same shared infrastructure employing the Cisco ASA routed virtual context as the default gateway for the web server. The construction of this structure is identical to the previously documented enclave except for the firewall mode of operation.

Figure 12. Enclave Model: Routed VLAN with VXLAN (Cisco ASA Routed Mode)

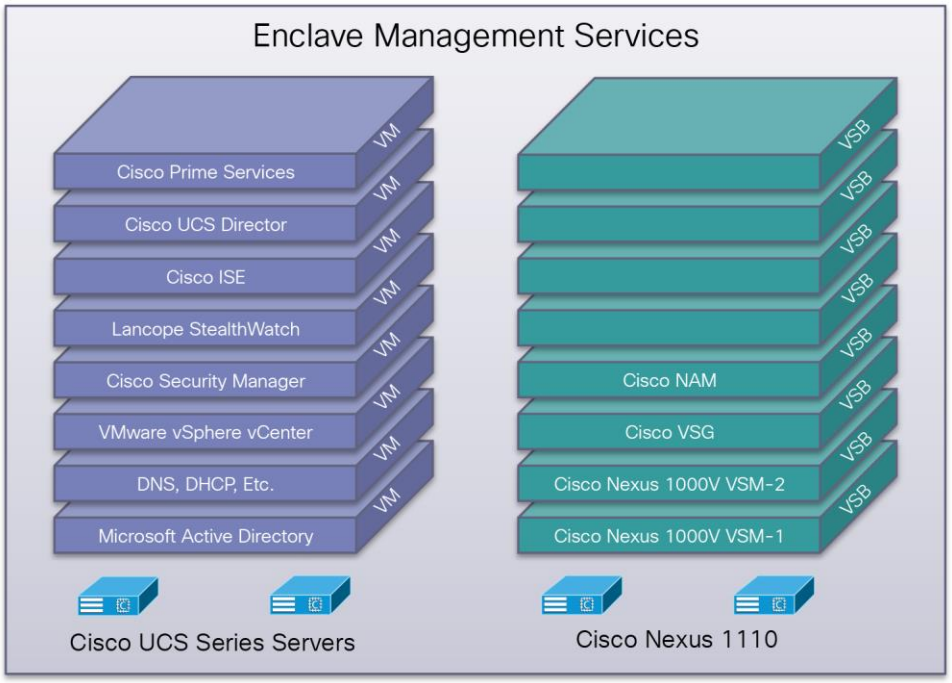


Enclave Management

The enclave management network is a dedicated Cisco converged infrastructure stack consisting of Cisco UCS servers and Cisco Nexus 1110-S Virtual Services Appliances, providing centralized access, visibility, and control of resources within the system. The management network supports domain- and element-level management to provide comprehensive administration of the shared resources that compose the Cisco Secure Enclaves architecture. The administrative interfaces and open APIs available in this management portfolio provide the foundation for delivery of cohesive service lifecycle orchestration with Cisco UCS Director.

Figure 13 shows the management services currently used in the design and their associated host platforms. In practice, multiple Cisco UCS servers, depending on the resource requirements of the installation, are deployed as part of the dedicated VMware vSphere HA and DRS cluster for management. The Cisco Nexus 1110 appliances support a number of virtual services blades (VSBs), including two instances of the Cisco Nexus 1000V Virtual Supervisor Module (VSM); one VSM services the production enclaves, and the other services the management domain. The Cisco VSG VSB provides Layer 2 security services to the virtual machines in the environment.

Figure 13. Enclave Management Services and Positioning



Note: The enclave framework is not restricted to the management services listed in Figure 13.

The communication between the management domain, the hardware infrastructure, and the enclaves is established through traditional paths as well as through the use of private VLANs on the Cisco Nexus 1000V and Cisco UCS fabric interconnects. The use of dedicated out-of-band management VLANs for the hardware infrastructure, including Cisco Nexus switching and the Cisco UCS fabric, is a common best practice. The enclave model suggests the use of a single isolated private VLAN that is maintained between the bare-metal and virtual environments. This private isolated VLAN allows all virtual machines and bare-metal servers to converse with the services in the management domain, which is a promiscuous region. The private VLAN feature enforces separation between servers within a single enclave and between enclaves.

Figure 14 shows the logical construction of this private VLAN environment, which supports directory, DNS, Microsoft Windows Server Update Services (WSUS), and other common required services for an organization.

Figure 14. Private VLANs Providing Secure Access to Core Services

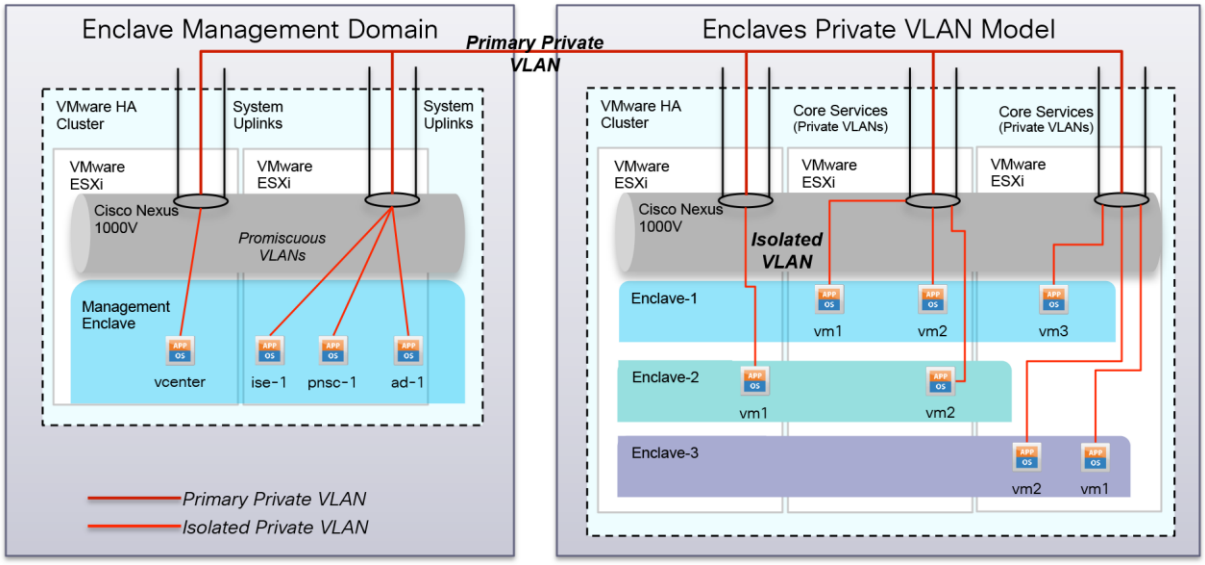
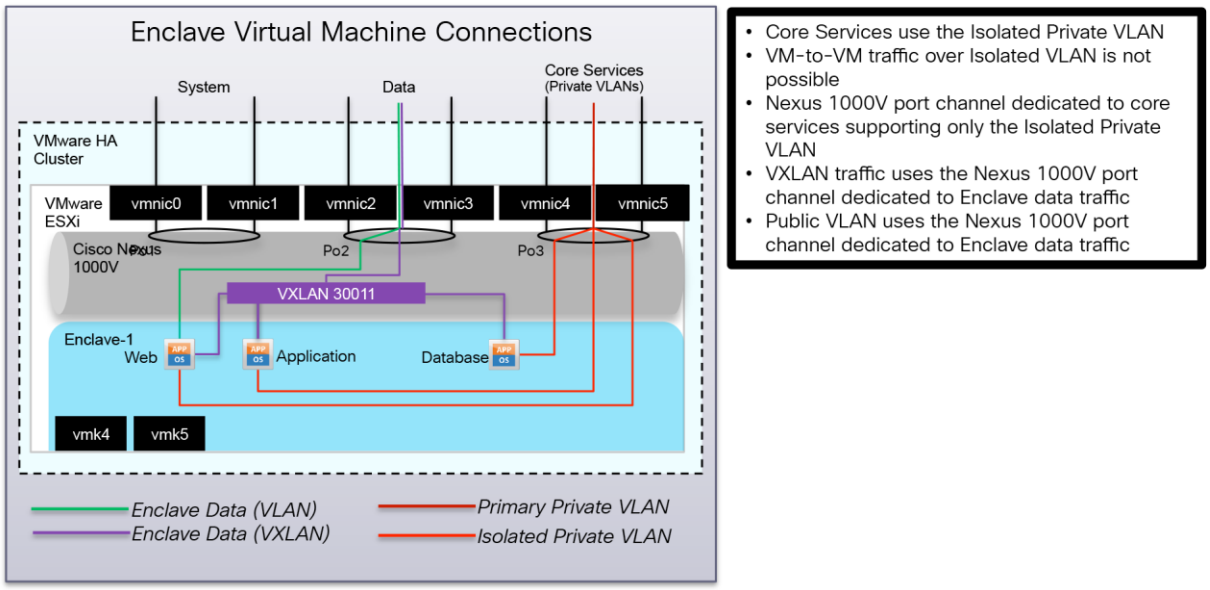


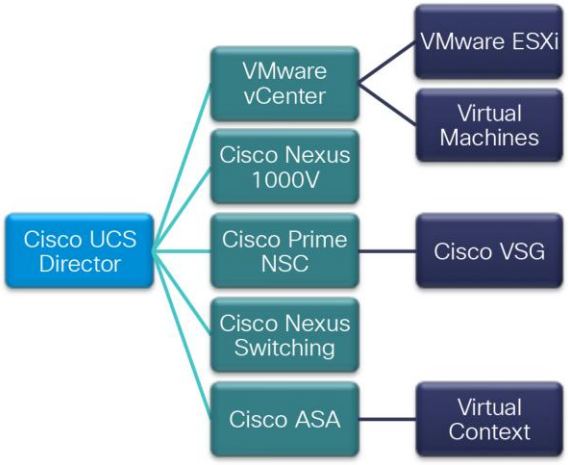
Figure 15 shows on the virtual machine connection points to the management domain and the data domain. As illustrated, the traffic patterns are completely segmented through the use of traditional VLANs, VXLANs, and isolated private VLANs. The figure also shows the use of dedicated PCIe devices and logical PortChannels created on the Cisco Nexus 1000V to provide load balancing, high availability, and additional traffic separation.

Figure 15. Enclave Virtual Machine Connections



Cisco UCS Director provides a central user portal for managing the environment and enables the automation of the manual tasks associated with the provisioning and subsequent operation of the enclave. Cisco UCS Director can directly or indirectly manage the enclave components. Figure 16 shows the interfaces that Cisco UCS Director employs.

Figure 16. Cisco UCS Director Enclave Control Framework



Traffic Patterns

Traffic patterns in the shared infrastructure can be divided into two categories: north-south (client to server) and east-west (server to server); see Figure 17.

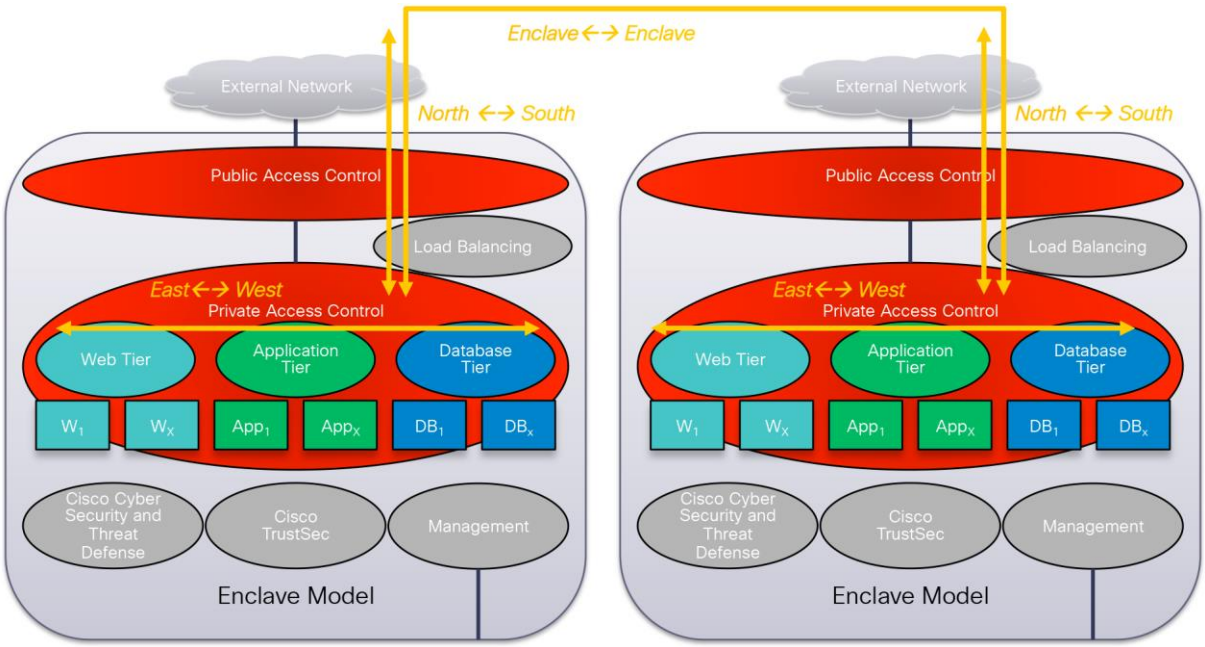
Client-to-Server (North-South) Flows

North-south traffic flows are either ingress or egress flows from the enclave perspective and are generally understood as being client-to-server in nature. This traffic traverses the enclave and is exposed to any number of services in its path, including firewalls, load balancers, intrusion detection, and network analysis devices in the enclave. In a multiple-enclave environment, traffic between enclaves (enclave-to-enclave traffic) is also considered north-south in nature and therefore is subject to each enclave's independent policies as it progresses.

Server-to-Server (East-West) Flows

East-west traffic refers to the communication between servers within an enclave. This more focused view of this horizontal traffic pattern allows administrators to hone and refine the policies within the enclave. Firewalling, load balancing, and threat defense can be tuned to meet the application requirements within the enclave.

Figure 17. Enclave Traffic Patterns



Design Considerations

The key to developing a robust design is clearly defining the requirements and applying a proven methodology based on sound design principles of:

- Protection
- Performance
- Provisioning
- Availability
- Service assurance

A framework that provides secure administrative and user-domain protection with application-level service assurance through quality of service (QoS) delivered by dedicated high-performance appliances on a highly available platform constitutes the foundation on which complementary products can be deployed to provide customer-specific features. Another essential component of such a design is automation of resource provisioning to provide operation efficiency and help ensure implementation accuracy.

Protection

Given the borderless nature of users and access methods currently in use, the security mechanism needs to be ubiquitous (defense in breadth) and deep (defense in depth) to eliminate both circumvention and penetration, which can lead to intrusion. Cisco ASA firewalls serve as the first line of defense for both ingress and egress traffic to and from the enclave. Cisco VSG integrated into the Cisco Nexus 1000V is a virtual firewall that provides distinct trust zones on shared computing infrastructure for east-west traffic between virtual machines. Together, the Cisco ASA firewall and Cisco VSG provide protection against perimeter attacks as well as internal attacks. This

comprehensive protection safeguards against disruptions to critical administrative functions of the cloud infrastructure so that valuable shared user-domain resources are protected.

Access to resources such as virtual machines, network bandwidth, data, and storage needs to be curtailed at both the logical and physical levels, where possible, to impose necessary controls. Protection against denial-of-service (DoS) attacks and unauthorized access leading to data loss is delivered through the threat analysis and zero-day protection features of Lancope StealthWatch.

Preservation of user-space confidentiality through encryption and other means at multiple levels through use of access controls, virtual storage controllers, VLAN segmentation, firewall rules, and intrusion protection should be employed where possible. Data protection through continuous encryption of data in flight and at rest is essential for integrity. Cisco TrustSec SGT support on most Cisco devices is crucial to enabling proper access control in a distributed manner for a scalable and secure platform. Assessing the efficacy of the implementation and adapting to defend against new and evolving threats require continuous and comprehensive visibility into the operations of the network and its components. Cisco NetFlow implementations along with flow analysis by Lancope StealthWatch are invaluable in this area. Together, Cisco NetFlow and Cisco TrustSec deliver visibility and control, which are essential for an open and secure platform.

The enforcement module with Cisco TrustSec and Cisco NetFlow extends its reach into underlying networking, computing, storage, and management components within this architecture to provide features and capabilities that together provide a trusted environment.

Performance

Delivery of security involves consumption of computing resources. Providing security in a consistently responsive manner requires even more resources from potentially a shared pool that may be needed by hosted applications. Although these resources may appear as overhead, user confidentiality is essential. Thus, organizations need to implement secure services that are scalable with the least overhead. Previously discussed design principles such as the least-common mechanism and efficient mediated access are shown to provide guidance in devising a platform that delivers on these needs. The goal is to provide sufficient performance to help ensure that the necessary security checks are performed within the permitted time and before the user experience becomes a concern.

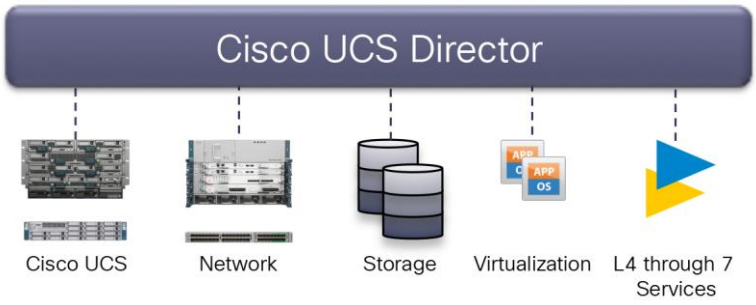
To this end, the high throughput of Cisco ASA firewalls and Cisco NetFlow appliances with managed device capabilities removes overhead from the underlying shared platform used by hosted applications. This design methodology also leads to a scalable cluster of firewalls and Cisco NetFlow devices that can grow to accommodate the needs of the enterprise with a secure and separate enforcement module that conforms to the reference monitor. Virtual PortChannel (vPC) technology on both physical and virtual implementations of Cisco Nexus switches provides link-layer resiliency and additional bandwidth as needed.

Provisioning: Ease of Management

Provisioning design includes such features as rapid and correct provisioning for easy adoption and for effective management of resources. Domain and element management provides comprehensive administration of the shared resources that compose the secure cloud architecture. The demarcation point for managing components in this design is defined by individual programmable interfaces delivered by Cisco and partner products. The administrative interfaces and APIs in this portfolio address infrastructure components such as VMware vCenter, Cisco UCS Manager, Cisco Data Center Network Manager (DCNM), and storage managers. These element managers and their associated open APIs provide the foundation for delivery of cohesive service lifecycle

orchestration with Cisco UCS Director. At a logical level, Cisco UCS Director integrates infrastructure components into a single management pane (Figure 18).

Figure 18. Cisco UCS Director Abstracts Infrastructure Layers into a Single Management Pane



High Availability

High availability helps ensure that systems and data are available and accessible to authorized users when they are needed by introducing redundancy at every layer of the infrastructure: computing, network, and storage. One other desirable outcome of the elimination of single points of failure is a setup that allows planned maintenance with little or no disruption in most cases. Each layer has its own way of providing a highly available configuration that works transparently with adjacent layers.

Service Assurance

Service assurance requires available controls and components to help ensure that the SLAs expected from the platform, including security, are met. The components and features necessary to deliver agreed-on system performance pertaining to underlying components such as computing, networking, and storage resources during both steady-state and non-steady-state environments are covered. For example, the network and Cisco UCS blade architectures can provide detailed bandwidth guarantees using QoS; resource pools in VMware help balance and guarantee CPU and memory resources, while comparable features at the storage level support declared I/O operations per second (IOPS) deliverables.

Conclusion

The Cisco Secure Enclaves architecture uses the common components of Cisco Integrated Systems with additional services integrated to address business and application requirements. These functional requirements promote uniqueness and innovation in the integrated computing stack, augmenting their original design with support for essential services such as security and manageability. The result is an a region, or enclave, and more likely multiple enclaves, within the integrated infrastructure designed and built to appropriately address the unique workload activities and business goals of an organization. This design and the validation discussed here shows the benefits of secure enclaves in Cisco's integrated stacks.

For More Information

- Lancope NetFlow Bandwidth Calculator: http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/
- Cisco NetFlow Performance Analysis: http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd80308a66.pdf
- Cisco TrustSec Solution 2.0 Design and Implementation Guide: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf
- Cisco Cyber Security and Threat Defense Solution 1.1 Design and Implementation Guide: http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/cyber_threat_defense_design_guide.pdf
- Gaining Visibility and Context Through NetFlow Security Event Logging: http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/guide_c07-728135.pdf
- Gain Visibility into the Data Center with the Cisco NetFlow Generation Appliance: http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/guide_c07-728136.pdf
- Secure Data Center for the Enterprise Solution: http://www.cisco.com/go/designzone
- Design Principles for Security, by Terry V. Benzel, Cynthia E. Irvine, Timothy E. Levin, Ganesha Bhaskara, Thuy D. Nguyen, and Paul C. Clark http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476035
- Observations on the Effects of Defense in Depth on Adversary Behavior in Cyber Warfare, by Dorene L. Kewley and John Lowry http://www.bbn.com/resources/pdf/USMA_IEEE02.pdf
- Cisco Validated Designs consist of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments; see http://www.cisco.com/go/designzone

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C07-731204-00 03/14