Secure Separation Built on FlexPod Solution Overview

Last Updated: November 16, 2011

Secure Separation Built on FlexPod Solution Overview

Secure Separation Built on FlexPod Solution Overview

Introduction

Rapidly proliferating silos of servers, storage, and networking resources combined with numerous management tools and operational processes have led to rigidity, inefficiencies, and soaring costs in the traditional data center. Consequently, businesses are moving away from silos and moving toward a next-generation data center based on a shared, virtualized infrastructure that improves responsiveness, lowers costs, and ultimately enables the journey to to a private or public cloud. This next-generation data center must be optimized for virtual and cloud computing environments, be flexible enough to fit into their current infrastructure and easily adapt to a wide range of mixed workloads, and scale for tremendous future growth. The FlexPod™ data center solution has been developed to provide businesses with a unified, pretested, and validated shared infrastructure to simplify their data center transformation.

FlexPod is a data center platform from Cisco and NetApp that hosts infrastructure software and business applications in virtualized and non-virtualized environments. The platform has been tested and validated across leading hypervisors and operating systems from VMware, Red Hat, and Microsoft, and can be managed by FlexPod Ecosystem partner software. FlexPod scales to accommodate multiple workloads in a secure, multi-tenant environment.

Secure Separation Built on FlexPod is a capability that extends the FlexPod reference architecture to securely separate multi-tenant environments for non-virtualized workloads alongside virtualized ones. These capabilities make FlexPod an ideal application platform to deploy a wide range of application environments on a common, flexible, and manageable infrastructure.

Refer to Cisco's Design Zone for Data Centers (www.cisco.com/go/designzone/datacenter) for the complete series of Cisco Validated Designs for Data Center Virtualization featuring the Cisco Virtualized Multi-Tenant Data Center (VMDC). VMDC introduces the foundational architecture for deploying virtualized and multi-tenanted data centers for cloud-based services. It supports high availability, elasticity, and resiliency of virtualized compute, network, and storage services.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Benefits of Non-Virtualized Workloads on FlexPod

The secure separation capabilities broaden the deployment options for FlexPod by demonstrating how to securely separate workloads that do not require or do not plan on leveraging virtualization. The migration effort to FlexPod has been simplified since both virtualized and non-virtualized applications can be moved directly to FlexPod and run concurrently on the converged, common infrastructure.

Application environments that have virtualized and non-virtualized components now can be deployed and managed on a common infrastructure. Many applications are not suitable to be virtualized; thus, they can be deployed on FlexPod as a non-virtualized workload. Common reasons these applications remain non-virtualized include legacy applications that are not supported when run in a virtualized environment and unique application demands which require exclusive allocation of the server resources. For example, applications such as Oracle and SAP commonly have “resource hungry” database engines that in many cases continue to be deployed in non-virtualized environments to satisfy performance and resource requirements. Other software components, such as middleware and web servers, are virtualized and deployed as farms, front-ended by load balancers. Virtualized resources assigned to these components can spread horizontally and can be dynamically allocated to accommodate the varying demands placed on the application. Thus, an application platform built on FlexPod can concurrently support an application’s virtualized and non-virtualized resource needs, where some server resources are allocated to virtualized resources and others to non-virtualized ones.

The shared infrastructure is an ideal environment to house a wide range of custom applications. In most companies, it is common to find hundreds of custom applications that are targeted to be moved to the data center as part of the cost savings realized by data center consolidation initiatives. Many of these applications are not suitable to be virtualized; thus, they can be deployed on FlexPod as a non-virtualized workload. Common reasons these applications remain non-virtualized include legacy applications which are not supported when run in a virtualized environment, unique application demands which require exclusive allocation of the server resources, and IT decision makers not ready to adopt virtualization.

As part of a RISC migration strategy, FlexPod is an ideal target application platform. Current aging and proprietary RISC/UNIX infrastructure cannot provide the performance and the flexibility required to support rapidly changing business requirements and the cost to scale for additional performance is high. At a time when data centers are moving to cloud computing, there is a greater need for standard, non-proprietary platforms and solutions. Migrating to Red Hat Enterprise Linux offers the flexibility to run the applications you require without sacrificing the RAS features of enterprise UNIX or replacing or retraining administrative staff.

FlexPod delivers outstanding reliability, flexibility, and performance while lowering total cost of ownership (TCO). FlexPod’s flexibility to support a wide range of workload makes it an ideal platform as part of a RISC-to-x86 migration.

Technical Overview

FlexPod’s secure separation data center architecture provides a flexible service delivery framework that can be used to host multiple applications or services on the same infrastructure. In both virtualized and non-virtualized environments, the administratorss objective is to employ data center resources as efficiently as possible, while meeting the service level requests of each application. The myriad of applications within the shared data center infrastructure must, at a minimum, coexist and, if required, reliably interact as dictated by application or organizational requirements.

Multi-tenant data center design advances the notion of shared resources to provide the tenants (or organizations) with what appears to be a dedicated data center environment. The multi-tenant organizational policy must safeguard the integrity of each tenant, ensuring one tenant cannot impede on

the access of another tenant to their equitable share of data center resources. To achieve these goals, Cisco and NetApp have worked with Red Hat to implement securely separated non-virtualized tenants in a data center built on FlexPod.

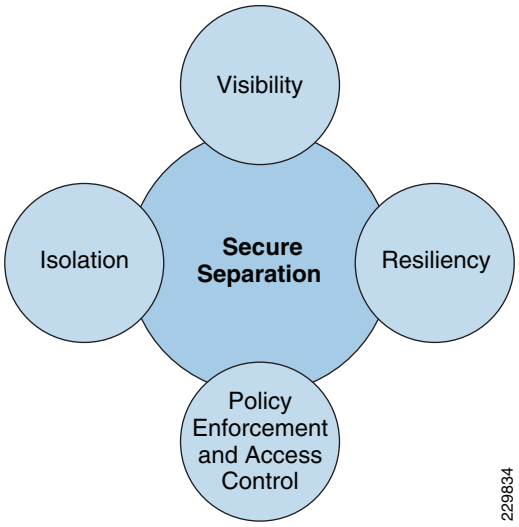
Organizational needs dictate the requirements for each tenant and between tenants and may be driven by business, compliance, or application requirements. The design is built on foundational components that create the environment for providing securely separated services. The specific requirements for each tenant determine how the foundational components are implemented to deliver the expected services.

The secure separation design ensures one tenant does not have access to another tenant's resources, such as operating system, network bandwidth, and storage. Each tenant must be securely separated from every other tenant and from other threats to the data center.

Secure separation is the partition that prevents one tenant from having access to another's environment and also prevents a tenant from having access to the administrative features of the infrastructure. The following briefly describes the main security principles that are implemented in this architecture.

- Isolation—Isolation can provide the foundation for security for the multi-tenant data center and server farm. Depending on the goals of the design, isolation can be achieved through the use of firewalls, access lists, VLANs, virtualization, storage, and physical separation. A combination of these can provide the appropriate level of security enforcement to the server applications and services within different tenants.
- Policy Enforcement and Access Control—Within a multi-tenant environment, the issue of access control and policy enforcement looms large and requires careful consideration. Capabilities of devices and appliances within each layer of the architecture can be leveraged to create complex policies and secure access control that can enhance secure separation within each tenant.
- Visibility—Data centers are becoming flexible in the way they scale to accommodate new services and new servers (both virtualized and non-virtualized). This architecture leverages the threat detection and mitigation capabilities that are available at each layer of the network to gather alarm, data, and event information and dynamically analyze and correlate the information to identify the source of threats, visualize the attack paths, and suggest and optionally enforce response actions.
- Resiliency—Resiliency implies that end-points, infrastructure, and applications within the multi-tenant environment are protected and can withstand attacks that can cause service disruption, data enclosure, and unauthorized access. Proper infrastructure hardening, providing application redundancy, and implementing firewalls are some of the steps needed to achieve the desired level of resiliency. Figure 1 shows the security architecture framework implemented in this design.

Figure 1 Security Architecture Framework



Core Components

The pre-validated Secure Separation Built on FlexPod architecture is built on the following components:

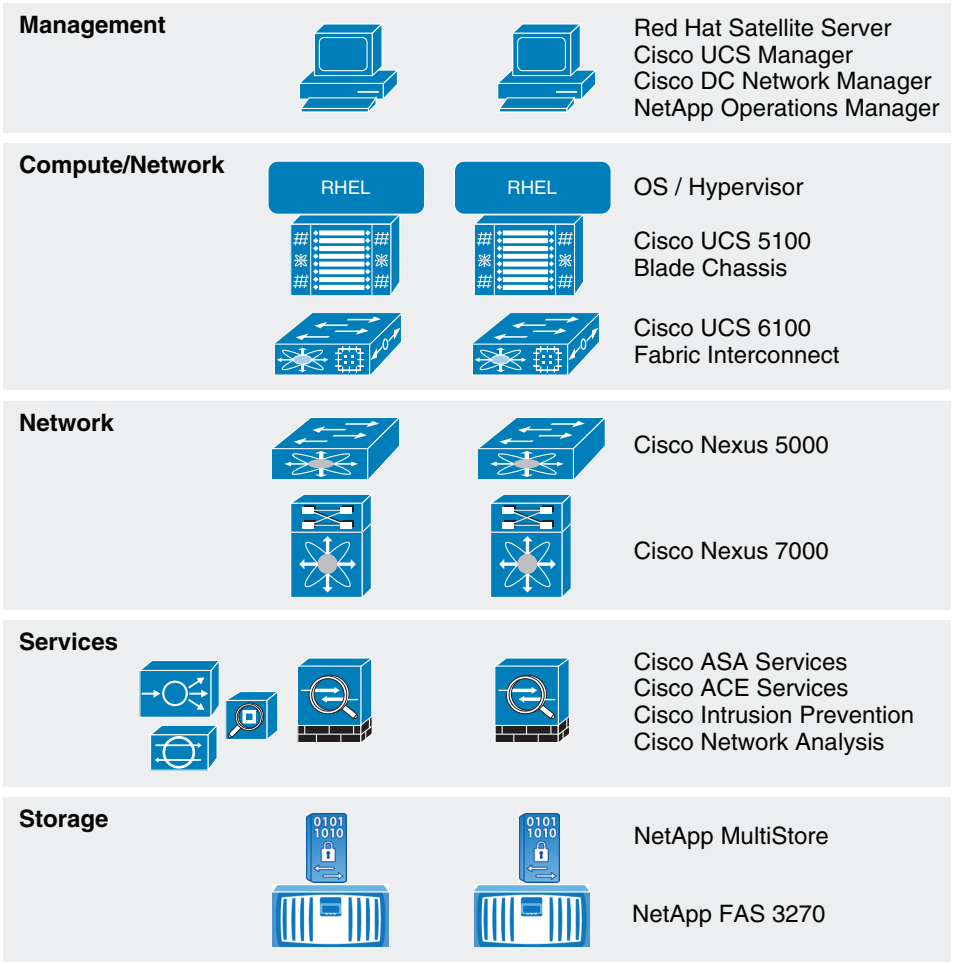
- Cisco Unified Compute System (UCS)
- Cisco UCS Manager
- Cisco Nexus 7000
- Cisco Nexus 5000
- Cisco Adaptive Security Appliance (ASA)
- Cisco Application Control Engine (ACE)
- Cisco Intrusion Prevention System (IPS)
- Cisco Network Analysis Module (NAM)
- Cisco Data Center Network Manager (DCNM)
- Cisco Application Network Manager (ANM)
- Cisco Security Manager
- NetApp FAS Unified Storage

Additional Components

Cisco and NetApp have worked with Red Hat to implement securely separated non-virtualized tenants in a data center built on FlexPod. The FlexPod environment in this solution also includes:

- Red Hat Enterprise Linux
- Red Hat Network (RHN) Satellite

Figure 2 Architecture Components



Key Benefits and Capabilities

Secure Separation Built on FlexPod is a system design that securely separates tenants on a shared FlexPod data center infrastructure, while each tenant appears to have a dedicated data center.

FlexPod is designed as a highly-available environment that provides both active and standby redundancy in all components. Eliminating planned downtime and preventing unplanned downtime are key aspects in the design of the multi-tenant shared services infrastructure.

Each tenant receives what appears to be dedicated compute, network, and storage resources, as defined by the system administrator through service policies. In a non-virtualized compute environment, service assurance for each tenant is achieved by:

- Compute—Native OS is installed on a blade or cluster.
- Network—VLANs separate the traffic, firewalls ensure separation between tenants, and quality of service (QoS) ensures packets are delivered with the appropriate priority, based on policies implemented by the administrator.
- Storage—A unique vFiler is assigned to each tenant, which allows each tenant to appear to have a dedicated storage resource.

As multi-tenant environments grow, so do the challenges of managing them. The components in the secure separation system design have element managers with rich feature sets and open APIs, allowing for customization of configuration, monitoring, and process automation through third-party or independently-created interfaces. Red Hat Network Satellite is an easy-to-use systems management platform for your growing Linux infrastructure. Built on open standards, RHN Satellite provides powerful systems administration capabilities such as management, provisioning, and monitoring for large deployments. Satellite allows you to manage many servers as easily as you would one. This design enables businesses to build a management environment that meets their business needs.

Supporting FlexPod

NetApp and Cisco share a long history of support collaboration to resolve our joint customers' technical issues. With the launch of the FlexPod solution platform, we have established cooperative support, a strong, scalable, and flexible support model to address the unique support requirements of the FlexPod converged infrastructure solution. The cooperative support model leverages the combined experience, resources, and technical support expertise of NetApp and Cisco to provide a streamlined process for identifying and resolving a customer's FlexPod support issue—regardless of where the problem resides. Backed by joint training of technical support teams, joint technology investments, strong cross-company support engineer and management relationships, and documented escalation processes, NetApp and Cisco are committed to accelerating resolution of a FlexPod support case.

For Secure Separation Built on FlexPod, NetApp and Cisco extend the cooperative support model to address support cases requiring collaboration with additional FlexPod software vendors. By engaging with the Technology Support Alliance Network (TSANet), the industry's recognized leader for effective multi-vendor support management, NetApp and Cisco can leverage TSANet's established interoperability support framework. It provides FlexPod partners a ready-to-use, scalable, operation infrastructure to address and resolve FlexPod cross-technology support issues quickly and efficiently.

Summary

Businesses are moving away from silos and moving toward a next-generation data center based on a shared, virtualized infrastructure that improves responsiveness, lowers costs, and ultimately enables the journey to a private or public cloud. FlexPod provides a validated common building block for data center deployments, with the ability to scale horizontally and vertically to meet business demands and standard interfaces that enable flexibility and efficiency. Lowering the risk and enabling the journey are primary benefits FlexPod provides businesses along this journey.

Secure Separation Built on FlexPod and the entire FlexPod series of design and deployment guides provide businesses with confidence and agility to deploy their cloud ready infrastructure. Comprehensive technical documents based on thousands of hours of testing, along with professional services and unified support, simplify the task of deploying these systems. Thus, business can quickly, safely, and confidently realize the benefits of running any of their workloads on a common, shared data center infrastructure.

For more information, see: http://www.cisco.com/go/flexpod.