Cisco Virtualized Multi-Tenant Data Center Cloud Consumer Models

Last Updated: March 6, 2012

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Virtualized Multi-Tenant Data Center

VMDC Cloud Consumer Models

An organization's IT environment faces many challenges to deliver cost-effective and efficient services that are responsive to current and future business needs. To address underutilized legacy systems with insufficient interoperability and integration capabilities to procurement timetables that delay service delivery, IT departments are looking to the cloud for solutions. Cloud deployment models are attractive to organizations as the potential benefits include:

- Organizational flexibility
- Reduced cost of infrastructure
- Agile and rapid deployment
- Relocation of IT resources
- New business models

Potential benefits mean there are no guarantees. Therefore, an organization should adopt a structured approach to their cloud projects that meets all requirements and concerns of their stakeholders, reduces risk, and realizes the potential of the cloud.

The Cisco Virtualized Multi-tenant Data Center solution (VMDC) is an architectural approach to IT that delivers a cloud-ready infrastructure. The architecture encompasses multiple systems and functions to define a standard framework for an IT organization. Using this standard, an organization can achieve operational efficiencies, reduce risks and costs while offering a consistent platform for business. Cisco's VMDC provides the following high-level benefits:

- **Reduced Time to Deployment**—Provides a fully tested and validated architecture that accelerates technology adoption and rapid deployment.
- **Reduce Risk**—Enables enterprises and service providers to deploy new architectures and technologies with confidence.
- **Increased Flexibility**—Enables rapid, on-demand, workload deployment in a multi-tenant environment using a comprehensive automation framework with portal-based resource provisioning and management capabilities.
- **Improved Operational Efficiency**—Integrates automation with multi-tenant resource pools (compute, network, and storage) to improve asset use, reduce operational overhead, and mitigate operational configuration errors.

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

The enterprise architecture affects how an organization creates and delivers value. Cisco VMDC defines how an organization can apply technology and processes to deliver value, coupling IT to the organization's overall business strategy. Cisco VMDC enables organizations to build the infrastructure foundation necessary to support a highly efficient, consistent, and easily scaled delivery model that unleashes the potential of the cloud.

Document Goal

The purpose of this document is to provide insight into the consumption models validated in Cisco's cloud ready infrastructure, VMDC. Adopting the National Institute of Standards and Technology (NIST) taxonomy and reference models provides a common nomenclature and starting point to address cloud services and technologies in any organization. NIST defines a Cloud Consumer as "a person or organization that maintains a business relationship with, and uses services from, Cloud Providers" and a Cloud Provider is defined as "a person, organization or entity responsible for making a service available to interested parties." The cloud consumer is the key party in any cloud deployment, and its interaction with the cloud provider is the focus of this paper.

Note Cloud consumers are more commonly referred to as "tenants."

An essential characteristic of NIST's cloud computing definition is resource pooling. Cisco VMDC addresses the consumption of shared resources by defining cloud consumer models. These constructs enable the organization to uniformly deploy and apply policies to shared resources.

Note The VMDC cloud consumer model is scalable meaning an organization may have a single or multiple consumer instances (multi-tenancy) which often correlates to the cloud deployment models as defined by NIST.

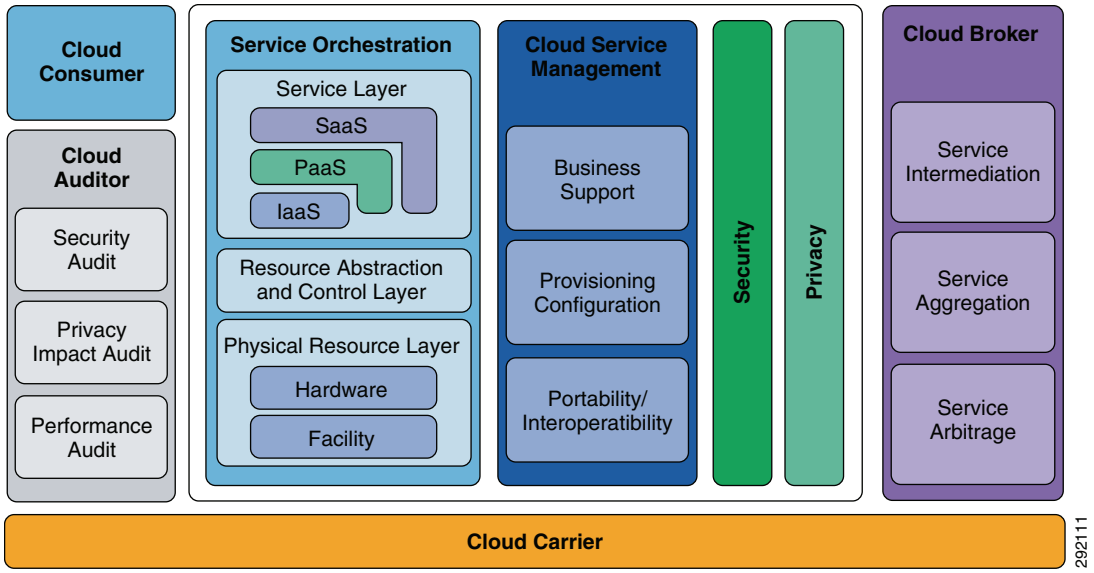
Audience

The target audience for this document includes both technical and professional stakeholders interested in the design of a cloud ready infrastructure delivering IT efficiency and enabling IT innovation to meet their overall business strategy.

Cloud Architectures

Cloud computing is best digested in a modular approach from its logical and physical components to the actors performing specific roles within the cloud environment. Figure 1-1 is the conceptual reference model defined by NIST illustrating the primary actors and their associated service or functions.

Figure 1-1 NIST Conceptual Reference Model of Cloud Computing



Source: NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture

Cloud Actors

The NIST defined cloud actors are cited in Table 1-1. It is beyond the scope of this document to define the interactions between each of these actors. The remainder of this document will focus on the opportunities that exist for cloud providers to satisfy cloud consumer demands.

Table 1-1 Definition of Actors in Cloud Computing

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	A entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Source: NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture

Note VMDC is a cloud-ready infrastructure built to address the resources, services, management, and security requirements of cloud providers.

Cloud Consumers and Providers

Cloud consumers use one or more services offered by cloud providers which are commonly categorized as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The availability, depth, and breadth of any one of these service offerings are determined by the cloud provider's business model. Regardless of the service model, cloud consumers will have service expectations and requirements encompassing availability, manageability, performance, security, as well as application and/or regulatory compliance. It is with these prerequisites in mind that cloud providers must address their infrastructure capabilities and cloud consumer models.

Cloud Deployment Models

NIST has identified four primary cloud provider deployment models, namely private cloud, public cloud, hybrid cloud and community cloud. The current definition for each of these approaches has been cited from NIST Special Publication 800-145, The NIST Definition of Cloud Computing.

- **Private clouds** are operated solely for one organization. They may be managed by the organization itself or by a third party, and they may exist on or off premises.
- **Public clouds** are open to the general public or to a large industry group and are owned and managed by a cloud service provider.
- **Hybrid clouds** combine two or more clouds (private or public) that remain unique entities but are bound together by technology that enables data and application portability.
- **Community clouds** have infrastructure that is shared by several organizations and supports a specific community. They may be managed by the organizations or a third party and may exist on or off premises.

It is important to note that although each of these models diverges in terms of cloud ownership or relative location of the cloud the underlying resources, services and functionality remain the same. The actors and their associated roles highlighted in Figure 1-1 are consistent. The cloud model is uniform.

VMDC Cloud Ready Infrastructure

Cisco's VMDC cloud ready infrastructure provides a structured approach to data center deployments from both a physical and logical perspective. The previous section discussed the principal actors and various deployment models associated with cloud computing. As shown in Figure 1-1, NIST Conceptual Reference Model of Cloud Computing, the cloud provider uses physical resources that are subject to various degrees of abstraction to deliver a service; IaaS, PaaS, SaaS.

VMDC is designed to meet the numerous demands required of a cloud environment and the models proposed by NIST. The following section will explore VMDC as a physical platform and the cloud provider consumer models that have been validated on this extremely flexible and consistent infrastructure.

The VMDC Platform

The VMDC physical infrastructure uses a combination of technology products and components to deliver cloud capabilities in a modular approach. This architectural consistency enables cloud providers to select the design that addresses their immediate needs, while providing a solution that can scale to meet future requirements without re-tooling or re-training staff. This scalability is based on two modular building blocks: the integrated compute stack (ICS) and point of delivery (PoD).

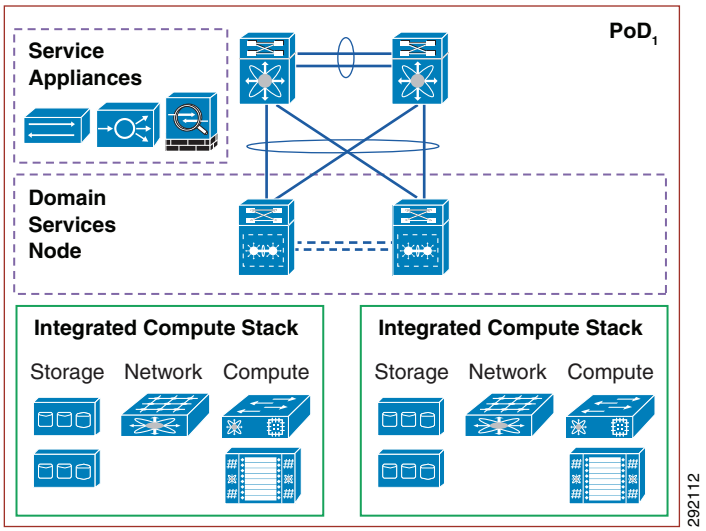
The integrated compute stacks consist of compute, storage and network elements that may support virtualized or non-virtualized workloads. The VCE Vblock and the Cisco NetApp FlexPod offerings are too such building blocks which may be readily introduced into the VMDC architecture. It should be noted that the VMDC architecture is not limited to any specific ICS definition but can be extended to include other compute and storage combination.

The PoD, or Point of Delivery, is another repeatable building block that allows organizations to deploy a uniform architecture. The PoD contains one or more ICS instances as well as intelligent network based services such as load balancing, firewalling, and intrusion detection. The PoD and ICS hierarchical design enables a predictable operational and scale model to the organization.

Figure 1-2 show the modular building blocks of the VMDC architecture. The ICS constructs and larger POD form creates a systematic approach to the physical deployment of the data center. Network services may be introduced via appliances or through service modules residing within a switching platform dedicated to network based service delivery in the PoD. Either option is valid and well documented within the VMDC solution allowing IT organizations to adopt the model which address their particular requirements without sacrificing functionality. The fundamental business drivers for adopting the PoD and ICS modularity are as follows:

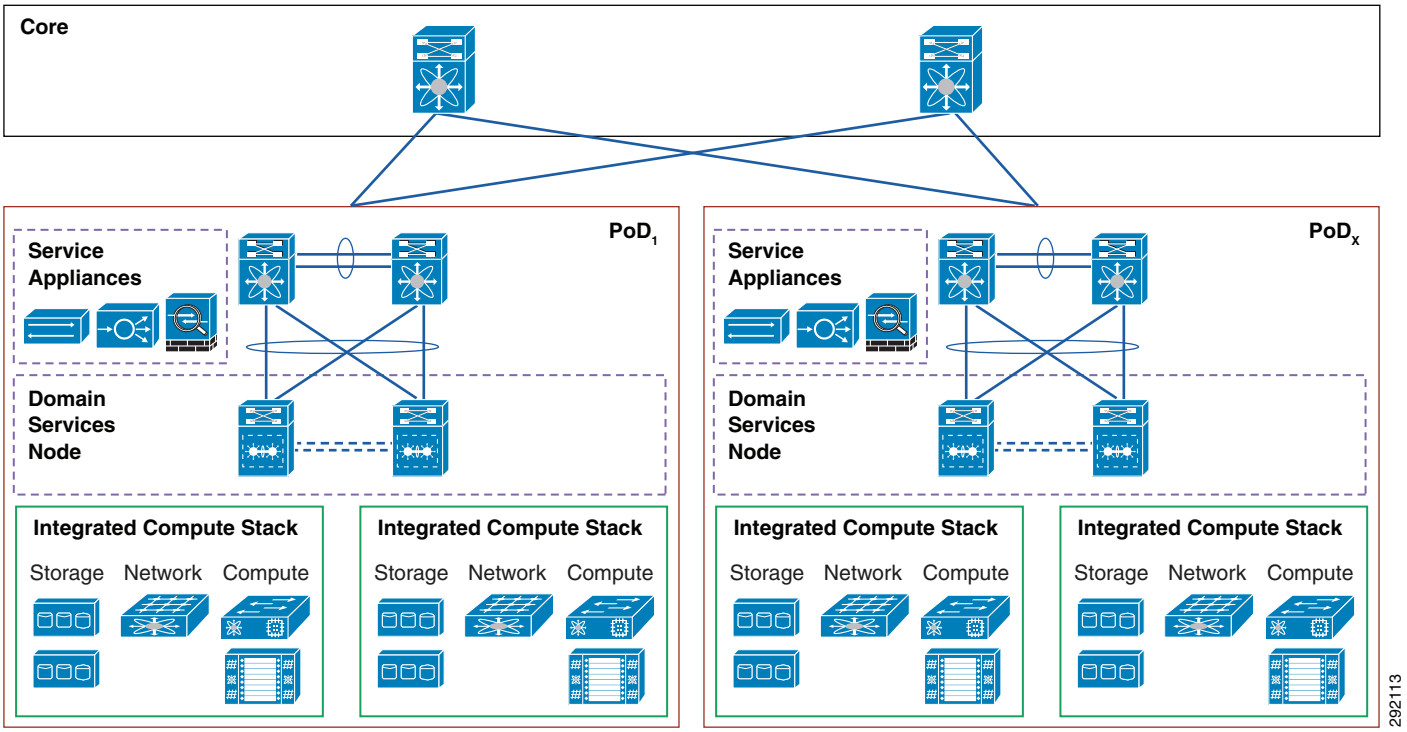
- Minimize operational impact, reduce TCO
- Flexible, multi-vendor architecture
- Pre-tested and validated IT infrastructure
- Architectural approach to cloud

Figure 1-2 VMDC POD and ICS Relationship



The PoD structure is a well formed unit of network, compute and storage capacity built to support the organizations business processes. If a single PoD reaches its performance limitation, the data center core may be leveraged to instantiate another PoD module within the data center. Since the VMDC building blocks are pre-defined, and their behavior well understood through Cisco's validation efforts, initial and future VMDC PoD rollouts become easier (Figure 1-3).

Figure 1-3 Scaling the VMDC PoD Structures with the Data Center Core



Note VMDC design and implementation details of the PoD and its validated scale can be found at http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

Cisco VMDC Cloud Consumer Models

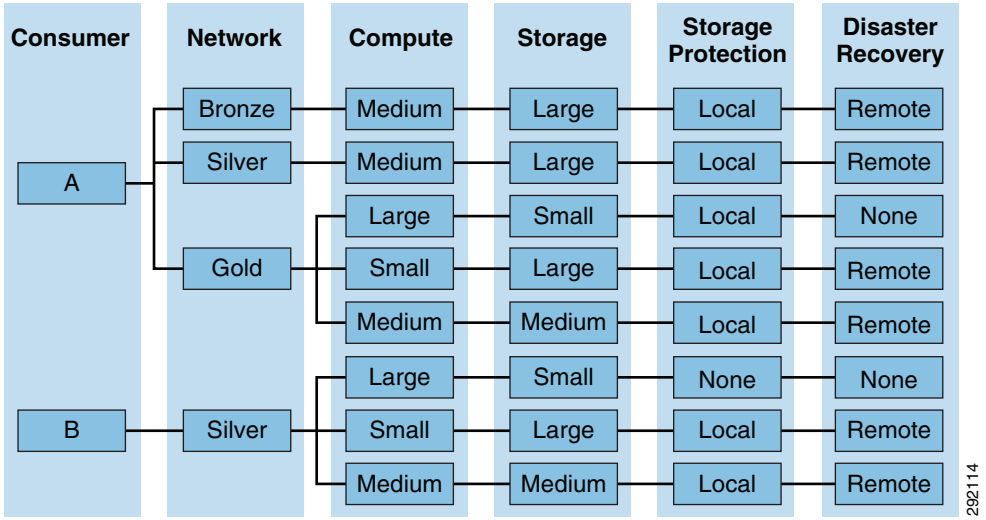
The cloud consumer is the key stakeholder for any cloud provider. This customer will require network, compute and storage resources of the provider. The cloud consumer will have varying availability, manageability, performance and security needs that must be addressed by the provider.

VMDC defines a consumption model enabling cloud providers to offer customizable cloud services using a standardized approach to meet their customers' particular business needs and expectations. This consumption model uses the previously defined VMDC shared infrastructure as its foundation. This section of the document will discuss the cloud consumer models validated within the VMDC cloud ready infrastructure and describe the compute, network and storage resource allocation framework.

Cisco VMDC Compute, Storage, and Network Approach

Cisco VMDC describes a cloud consumer model which accounts for storage, compute and network resources. At each technology layer, Cisco VMDC provides best practices and deployment guidelines to address cloud consumer service requirements which provide consumer isolation and system integrity at every level. The Cisco VMDC approach to resource consumption is to use three generic categories of storage and compute workload sizes. The compute small, medium and large classes address the processor and memory requirements of the server platforms, while the storage service levels reflect not only workload I/O options but data protection and recovery approaches. The network service offerings Gold, Silver and Bronze reflect a grouping of intelligent network services, security and quality of service combinations.Figure 1-4 shows two cloud consumers using various combinations of these service tiers. This example also reveals the intricacies of the cloud paradigm which Cisco VMDC simplifies through deployment best practices.

Figure 1-4 VMDC Service Tiering Example



Note For more details containing the VMDC service tier sizing details go to http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.0/large_pod_design_guide/Large_Pod_Design_Guide.pdf

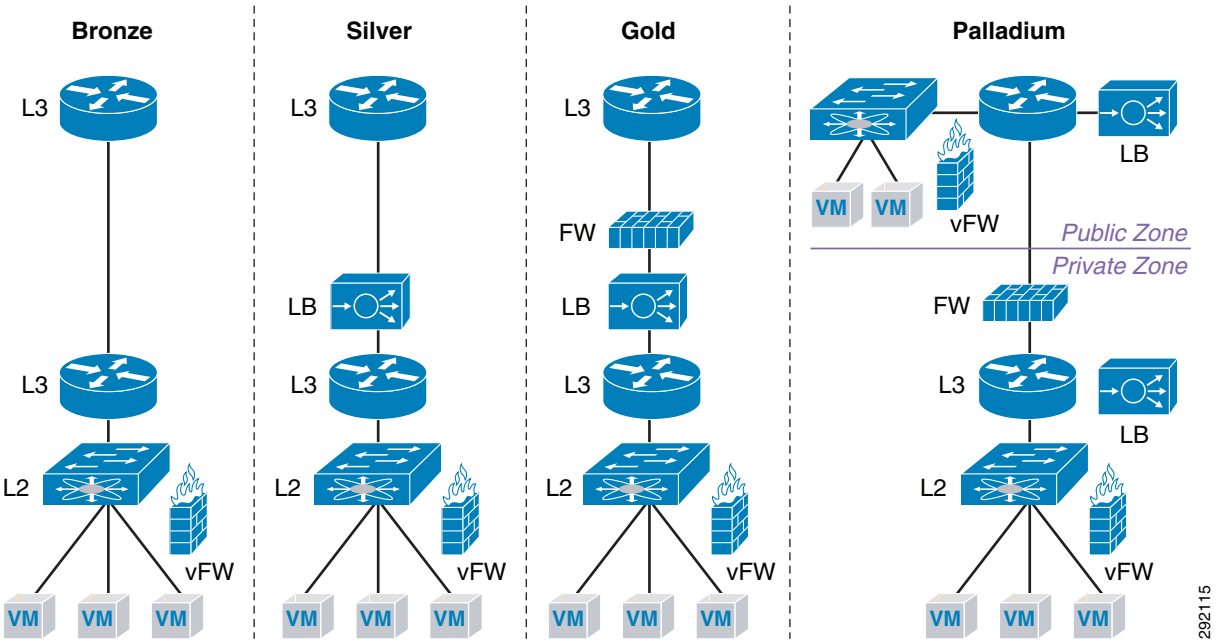
Network Service Tiers

The VMDC network service tiers are validated configurations which cloud providers may recommend to cloud consumers to support their specific workload requirements. These network templates define at a minimum Layer 2 and Layer 3 capabilities as well as supplementary application and security based services. Each of these service tiers provides logical separation of cloud consumers on a shared VMDC infrastructure. VMDC facilitates automation of this environment as it normalizes the deployment of network services within the cloud infrastructure which expedites cloud service delivery.

Figure 1-5 shows the logical configuration of the various network service tiers. Each network service tier uses network and network service virtualization to provide granular services to the cloud consumer. The Bronze tier is the simplest deployment option where fundamental network connectivity is enabled. Layer 2 and Layer 3 functionality is established. The Silver tier builds off the base stage as it offers

application availability and optimization services via the network while the Gold option provides enhanced security services within the network. The Bronze, Silver and Gold tiers are proscriptive models.

Figure 1-5 VMDC Cloud Consumer Network Models



The Palladium tier introduces the concept of two defensive zones referred to as Public or Private. The firewall is the border between these zones enforcing access control policies customized to the cloud consumer requirements. In addition, the Palladium design supports the deployment of a virtual load balancer in each zone for local application servicing. One important note, the VMDC Bronze, Silver, and Gold service tiers have very proscriptive implementation requirements. The Palladium tier however is more malleable allowing cloud providers to choose the manner in which security or application services are deployed. Please see the Cisco VMDC design zone page for the details.

Note The virtual firewall (vFW) instances highlighted above are optional to each network service tier model. The virtual firewall allows the introduction of defensive zones at the virtual access layer, but it is highly recommended to consider its implementation within the cloud.

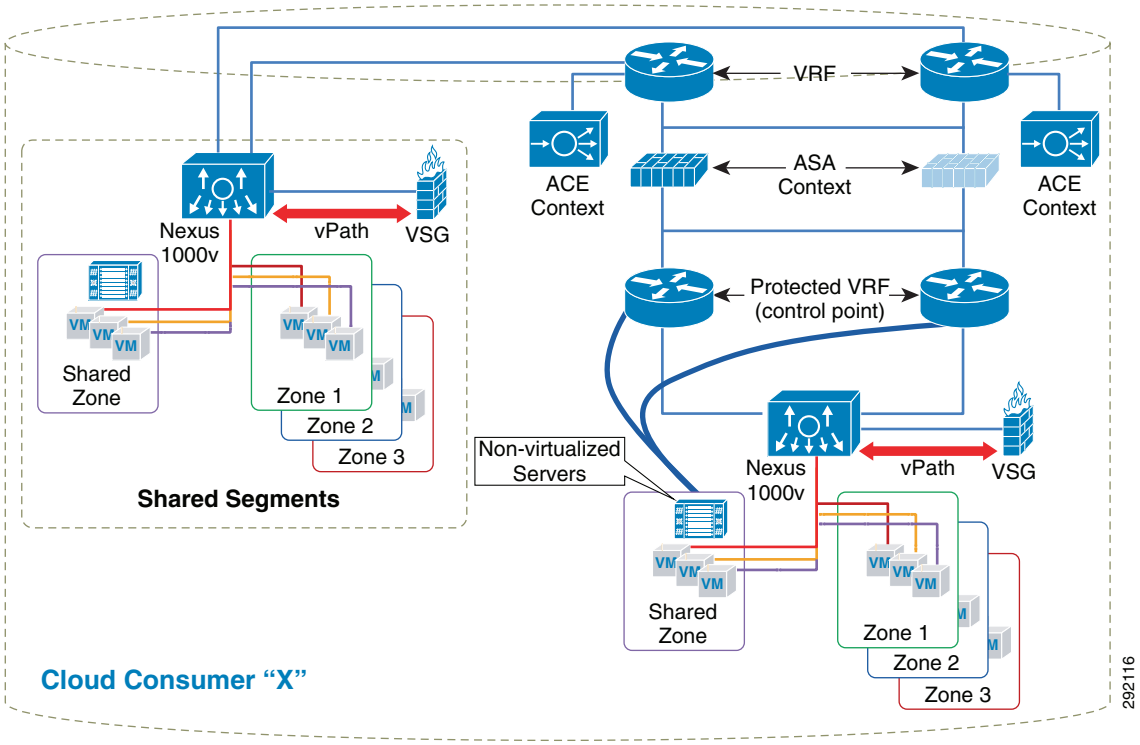
VMDC Cloud Consumer Modeling

The VMDC storage, compute and network service tiers are building blocks that culminate in a virtual data center environment capable of supporting one or many cloud consumers and their associated service requirements. The cloud consumer virtual data center or container allows a VMDC enabled cloud provider to replicate this logical structure in much the same manner VMDC allows the physical data center to be uniformly scaled via the ICS and PoD structures. The consumer virtual data center is a logical building block for the cloud provider and is captured in the Cloud Consumer Models illustrated below.

Figure 1-6 shows the VMDC cloud consumer container or virtual data center. The depicted model includes the network services described earlier. This component consists of virtual routers (VRFs), virtual firewall instances, virtual load balancers, as well as, virtualized and non-virtualized server platforms. The following highlights the form and function of this logical building block:

- The virtual machines employ the Cisco Nexus 1000V virtual switching platform.
- Security policies are enforced via the Cisco Virtual Security Gateway at the virtual access layer and virtual firewall context within the larger network.
- The FW context delineates the main “public” and “private” areas of the container as it enforces access control.
- The VSG may create multiple defensive zones within the virtual data center.
- The Protected VRF is a Layer 3 control point providing default gateway services.
- The virtual routing instance at the “top” of the container provides Layer 3 services and serves as a gateway for the Shared segments outside of the virtual firewall context.
- ACE load balancing virtual context are available for applications requiring their service.
- The Shared Segments section of the container may host common applications and data or provide a non-secure public presence to the container.
- Non-virtualized servers do not employ Cisco Nexus 1000V or VSG services. These servers rely on standard switching for Layer 2 services, but they do employ the services of the FW context.

Figure 1-6 VMDC Consumer Model



Note It should be noted that network analysis and intrusion detection and prevention devices may be readily added to this design. Please visit the VMDC Design Zone pages referenced below for more information.

Figure 1-7 shows a small variation of the VMDC cloud provider consumer model previously described. In this instantiation, the Shared Segments portion of the consumer’s virtual data center is secured by the firewall context services. This deployment option essentially creates a DMZ within the container.

Figure 1-7 Cloud Consumer Model with Secure Shared Segments

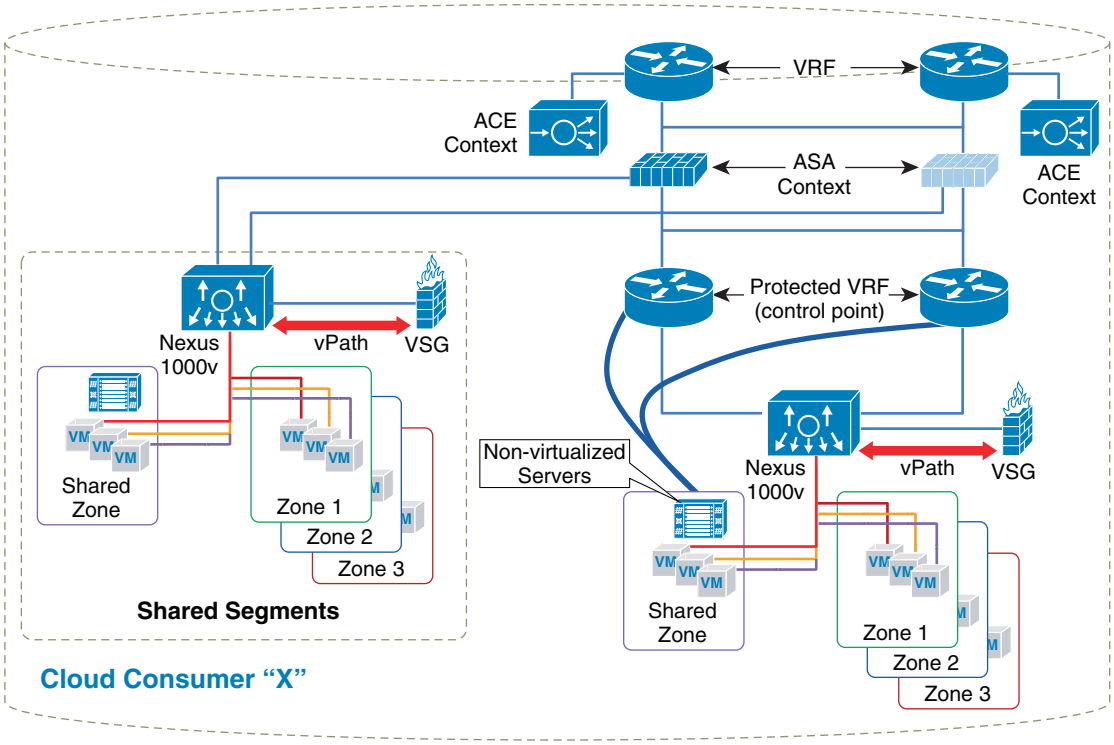
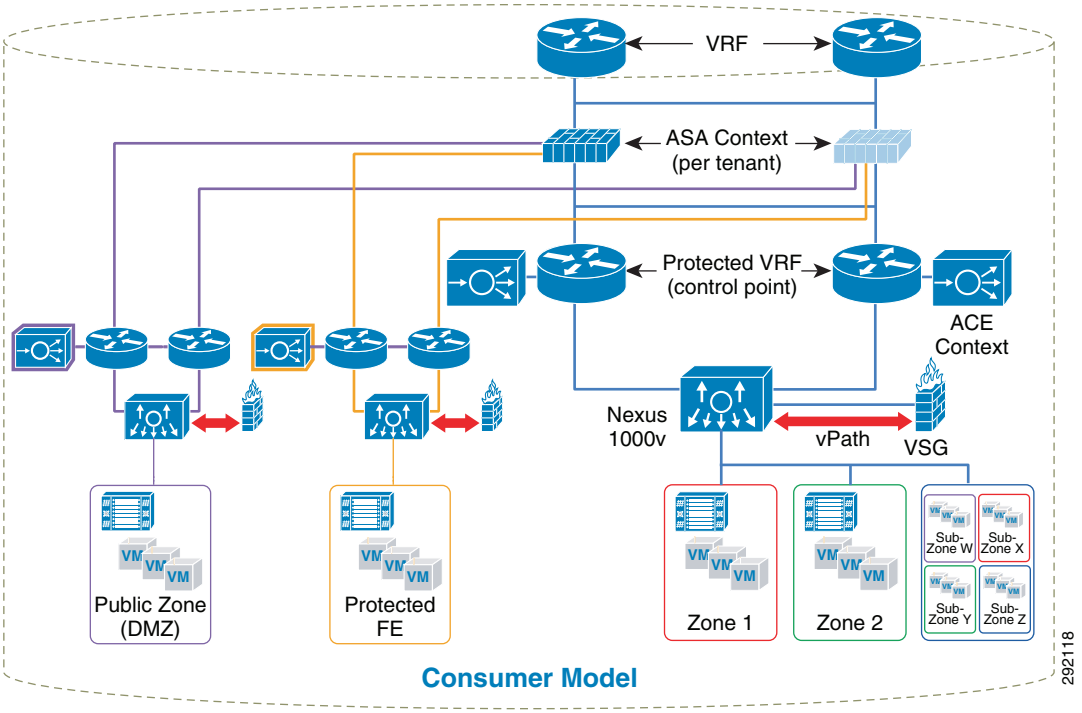


Figure 1-8 shows cloud consumer deployment within the VMDC cloud provider's environment. The consumer is leveraging the security services of the ASA virtual firewall context to create a more secure Public and Front-end environment for their users. In addition, unique Cisco Nexus 1000V and VSG instances provide Layer 2 connectivity and unique access control rules for their respective zones. Distinct ACE load balancing virtual contexts provide application availability and optimization features.

Zones 1 and 2 are also protected by the ASA virtual context and employ the Cisco Nexus 1000V and VSG for security policy enforcement. Distinct defensive zones for Web and Application tiers of a specific application have been creates as well as a dedicated data base zone. The third zone in this example is portioned into four defensive zones allowing this cloud consumer to further segment their virtual data center environment.

Figure 1-8 Consumer Model Example



Note Cloud consumers may also wish to be cloud providers, essentially a tenant may have sub-tenants. This model is supported by VMDC.

Traffic Pattern Implications

To create a complete cloud consumption model one needs to address the different traffic patterns existing within the environment. Recognition of these flows leads to the development and deployment of a comprehensive set of application and security policies. The traffic flows within the VMDC shared multi-consumer infrastructure can be divided into two distinct categories, north-south and east-west.

Consumer-to-Cloud—North-South Flows

North-south traffic flows are either ingress or egress in relation to the data center and are commonly understood as client-to-server in nature. This traffic traverses the data center and is readily exposed to any number of services in its path including firewalling, load balancing, intrusion detection, and network analysis devices. In the multi-consumer environment, traffic between consumers may also be forced through the data center network services. This functionality is ideal as each cloud consumer policy is uniformly applied between each other. The exposure of ingress-egress traffic flows to security services in the cloud provider's data center is dependent upon application specific requirements and the overall security policies of the enterprise.

In a cloud provider environment, different consumers may require different levels of service. Consumers with numerous requirements may require a host of virtual and physical appliances to satisfy their needs, while other consumers could benefit from a more basic service offering. For example, the human resource department would require a more stringent security infrastructure than the development-test organization. The capability to provide multiple levels of service as required and outlined in the VMDC Compute, Storage and Network Approach section is a unique attribute of Cisco's VMDC system.

Server-to-Server—East-West Flows

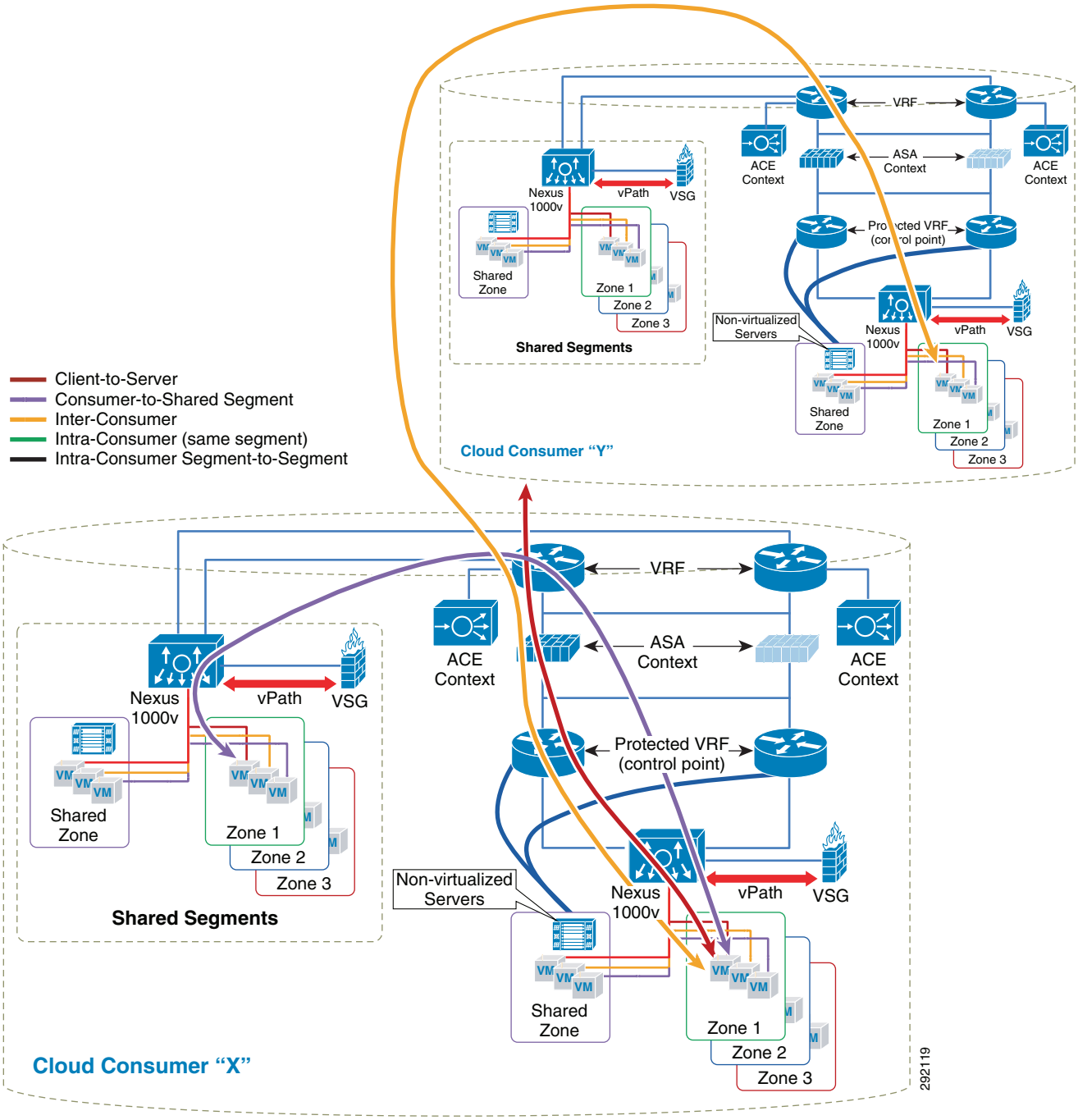
East-west traffic refers to the communication between servers within the data center access layer or virtual access layer; it is commonly referred to as server-to-server traffic. Securing inter-server communication can be an application-based requirement or an enterprise-based requirement. Typically, enterprise-class applications require more availability, scalability, and/or processing power than a single server instance can provide. To address these issues, application developers use dedicated server roles. Each role is specialized and dependent on other servers to complete their function. The VMDC consumer cloud model fully supports this application hierarchy. In the shared infrastructure of VMDC, server-to-server flows between virtual machines may occur within a single tenant container or between tenants.

To optimize east-west traffic patterns within a virtualized data center, it is recommended to use a virtual firewall appliance such as Cisco Virtual Security Gateway (VSG) to provide secure connectivity between virtual machines. This service may securely support intra- or inter-tenant communication. For example, a virtual firewall can provide secure connectivity for tenant virtual machines which need access to infrastructure services such as Active-Directory residing in the shared segments of the consumer's virtual data center.

Traffic flow Considerations for the VMDC Consumer Model

Figure 1-9 shows the traffic patterns within and between consumers within the VMDC based cloud. The design employs network services to create public and private zones which account for perimeter security and internal access controls. The internal zoning is enforced via the Cisco VSG allowing a single consumer to create multiple defense zones within and between application stacks or even sub-consumers within a single consumer virtual data center.

Figure 1-9 Cloud Consumer Traffic Patterns



Conclusion

The Cisco Virtualized Multi-tenant Data Center is a cloud ready infrastructure that is well suited to current cloud deployment models and cloud services. Cisco VMDC provides design and implementation best practices to de-mystify the cloud, offering a modular approach to the physical and logical operations of a cloud system. Combined with careful planning and execution, a VMDC-enabled IT organization can benefit from the cloud compute paradigm. As the cloud evolves, Cisco will enhance VMDC to address the future cloud requirements.

References

Cisco Design Zone:
http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html

Cisco Design Zone – Data Center Designs – Cloud Computing - VMDC

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

For more information about Cisco VMDC and access to the relevant documents, visit http://www.cisco.com/go/vmdc or contact your Cisco account representative.