Cisco Virtualized Multi-Tenant Data Center Services

At-A-Glance

Overview

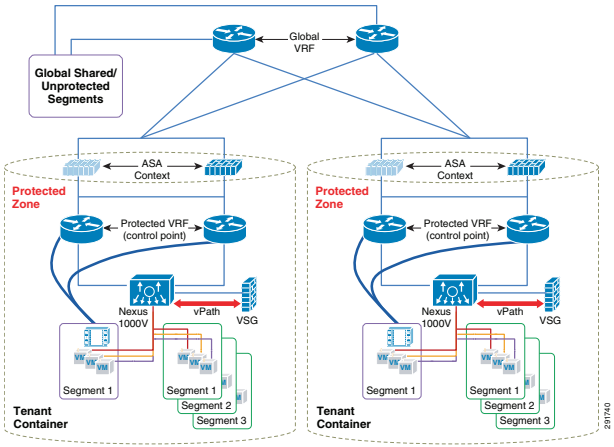
Cisco Virtualized Multi-Tenant Data Center (VMDC) is a validated reference architecture that delivers a highly-available, secure, flexible, and efficient data center infrastructure. VMDC provides the following benefits:

- Reduced time to deployment
- Reduced risk
- Increased flexibility
- Improved operational efficiency

Multi-tenancy enables business units, or compute environments that might have previously required separate security policies or entirely separate physical infrastructure to share physical resources, thereby reducing CAPEX and, the through resultant savings in power and footprint, OPEX.

The VMDC Tenant framework is modularized in a fashion that supports a single tenant deployment and is seamlessly expandable to a multi-tenant model without major reconfiguration or topology changes.

Figure 1 Extending the Model—Multi-Tenancy

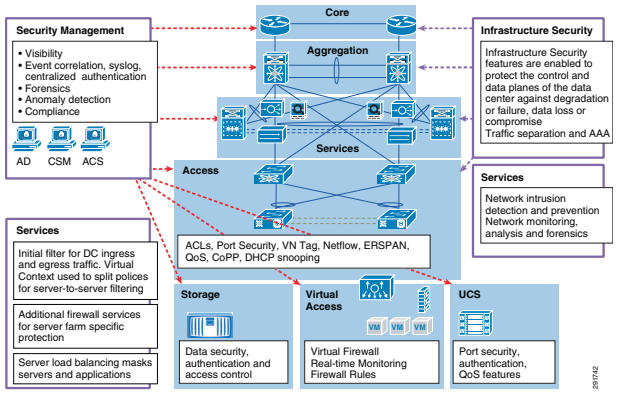


Data Center Services—Security Appliances

Cisco Unified Network Services is a key element of the Data Center Fabric, which addresses the need for dynamic, on-demand service delivery with consistently managed, policy-based provisioning. Cisco Unified Network Services brings integrated application delivery, network security, and network analysis to virtualized data centers and cloud environments as a key component of the Cisco Data Center Business Advantage Architecture.

The VMDC Reference Architecture provides an open, flexible model to integrate network services, allowing customers to readily integrate security and application-acceleration technologies as traditional physical service nodes (appliances) or virtual service nodes. This flexible approach to network-based services enables rapid and consistent deployment of solutions meeting specific application, security, or operational needs. VMDC employs a unified approach to application delivery, network security, and network analysis to virtualized data centers and cloud environments.

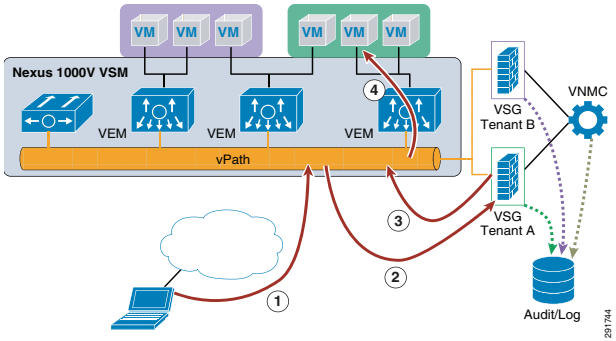
Figure 2 Security Control Framework



Cisco Virtual Security Gateway

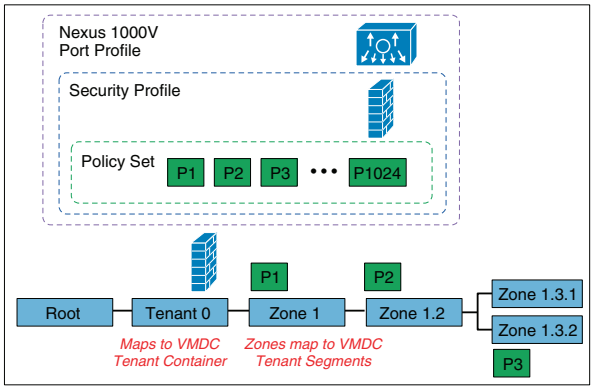
The Cisco Virtual Security Gateway (VSG) is a virtual security appliance that is tightly integrated with the Cisco Nexus® 1000V distributed virtual switch. The VSG uses the virtual network service path (vPath) technology embedded within the Nexus 1000V Virtual Ethernet Module (VEM). The vPath capability within the Nexus 1000V offloads the switching logic directly to the host, providing high performance, seamless interaction with other virtual appliances, and resiliency in case of appliance failure.

Figure 3 VSG Traffic Steering



VSG is designed to support multi-tenant environments and maps into VMDC quite seamlessly. The flexibility of the VSG tenant organization structure supports the open requirements for the tenant segment definitions within the VMDC framework.

Figure 4 VSG Linkage to Cisco Nexus 1000V



Cisco Prime NAM

A new version of the Cisco NAM—Cisco Prime NAM—is now offered in a virtual appliance form factor. Cisco Prime NAM offers traffic and performance analysis capabilities that empower network administrators to quickly troubleshoot performance issues and ensure optimal use of network resources in the Virtual Machine (VM) network.

Integrated with the Cisco Nexus 1010 Virtual Services Appliance, Cisco vNAM reduces network footprint, offers ease of deployment, and lowers administrative cost.

With Cisco Prime NAM, in conjunction with ERSPAN and NetFlow implemented on the Cisco Nexus 1000V, the following functions can be performed:

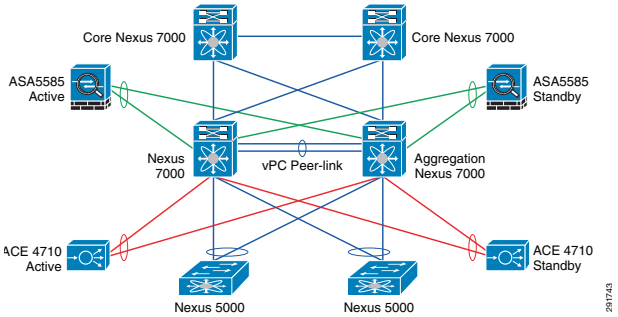
- Analyze network usage behavior by application, host/VM, and conversation to identify bottlenecks that may impact performance and availability
- Troubleshoot performance issues with extended visibility into VM-to-VM traffic, virtual interface statistics, and application response times
- Improve the efficiency of your virtual infrastructure with deeper operational insight

Appliance Deployment Options

Appliance versions of security and load balancing products are not new, but guidance on how to best integrate them into the VMDC Reference Architecture is a new addition to the design. An open, standard model is recommended for physical connectivity of the appliances that utilize LACP-enabled virtual port-channels (vPC) for link aggregation with 802.1q VLAN trunking.

This way inbound and outbound traffic flows to and from the appliance can be easily configured and controlled while benefitting from link aggregation resiliency and bandwidth.

Figure 5 Aggregation Layer Service Deployment Example (Excluding Failover Links)



Adaptive Security Appliance

The Cisco ASA 5500 Series IPS Edition provides best-in-class firewall, application security, and intrusion prevention capabilities in a single platform to defend the VMDC infrastructure from attack. Each tenant employs a dedicated Cisco ASA 5500 Series virtual context for explicit protection.

Application Control Engine

Cisco ACE 4710 technologies enhance application availability, accelerate application performance, and help secure the data center and mission-critical applications from attacks. VMDC tenants may reserve an ACE virtual context to meet their specific application needs.

For More Information

- VirtualizedMulti-Tenant Data Center New Technologies—VSG, Cisco Nexus 7000 F1 Line Cards, and Appliance-Based Services
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.6/vmdctechwp.html
- VMDC Design Zone
  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html