Cisco Secure Network Container: Multi-Tenant Cloud Computing

What You Will Learn

Cloud services are forecast to grow dramatically in the next 5 years, providing a range of features and cost benefits for customers and significant new revenue for service providers. Configuring, provisioning, and orchestrating cloud services that span networking, computing, and storage resources, however, is a complex and time-consuming challenge.

This document provides an overview of a new approach to the provisioning of cloud services: a service definition that encompasses network resources called Cisco® Secure Network Container. The Cisco Secure Network Container solution allows network administrators to configure physical and virtual network infrastructure and network services through templates that enable a level of abstraction. After the service definition has been created, these network services can interoperate with computing and storage resources to deliver end-to-end cloud services, enabling differentiated network services.

Challenges to Cloud Services Automation and Provisioning

The concept of cloud computing has gained global recognition over the past few years, but only now are data centers being redesigned to incorporate cloud attributes in a significant way. Data centers are consolidating architectures, adding virtualization, enabling services on demand, and developing build-as-you grow capability. Yet many challenges to the provisioning of cloud services remain.

Server teams recognize the opportunity of using virtualization to break down the silos that keep applications from sharing infrastructure and contribute to chronic underutilization of computing resources. However, their networking counterparts are typically not involved with some of the services necessary to orchestrate a cohesive cloud computing experience. Network services such as partitioning, logical isolation, firewalling, and application delivery are typically not enabled in a virtualized environment. The prevailing view is that these value-added services are too difficult to integrate into the network, or if they are integrated they will reduce the mobility and flexibility that hypervisor technology offers. The automated provisioning of applications with optimization rules that require complex integration increases the time needed to deploy a highly virtualized cloud. Until now, therefore, most service automation solutions have been offered for use with nonmobile, nonvirtualized applications.

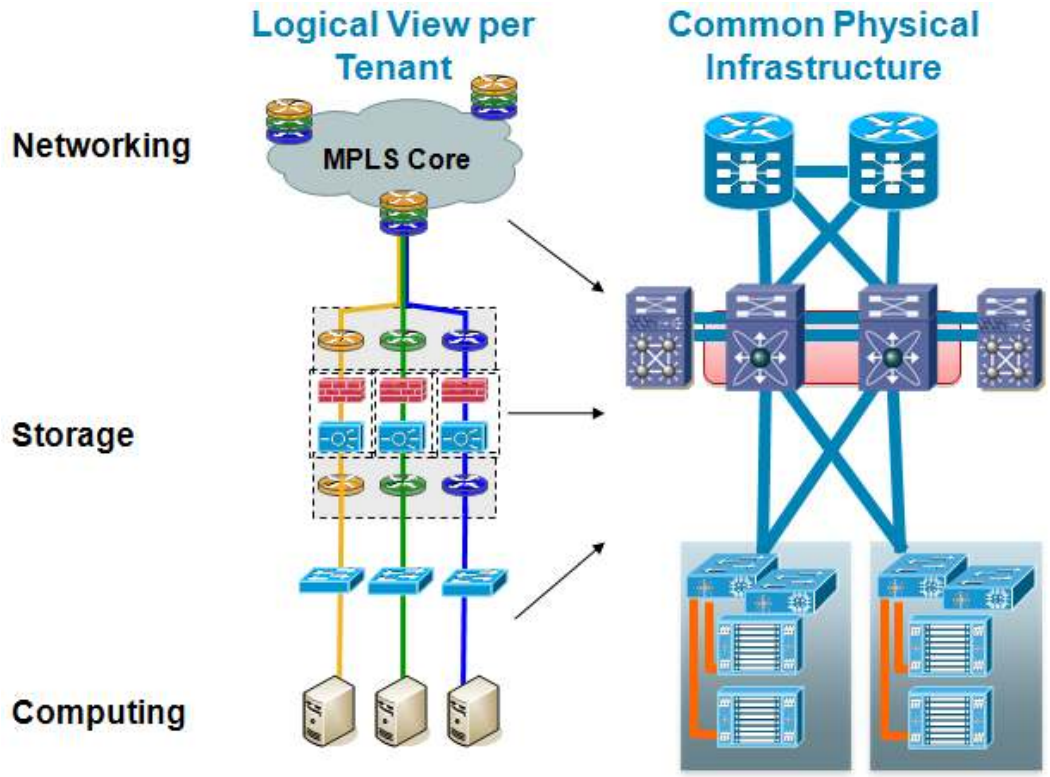
To offer infrastructure as a service (IaaS), software as a service (SaaS), or platforms such as the Cisco Hosted Collaboration Solution, service providers need a better way to automate and provision services across networking, computing, and storage resources. Simplifying and accelerating service provisioning and offering customers more choice among service attributes will differentiate service providers that offer these benefits from those that offer only services with a one-size-fits-all approach.

A new approach to the simplification and acceleration of service automation and provisioning is now available. It is expected to influence the movement of many business-critical services and applications to the cloud infrastructure in coming years. New confidence in the capability to automate, provision, and orchestrate secure virtual and physical resources in the data center will help promote the growth of cloud services, which in 2010 Gartner Research forecast to grow from US$58.6 billion in 2009 to US$148.8 billion by 2014 globally. Underlying this forecast is the perception among customers that cloud services are solutions that can deliver functions at lower cost and with more agility than traditional IT offerings.

Cisco Secure Network Container

For service providers with Cisco infrastructure, Cisco Secure Network Container allows network administrators to quickly and easily configure physical and virtual network infrastructure and network services to interoperate with computing and storage resources. Cisco Secure Network Container uses a level of abstraction within a network container template that consists of a set of virtual network resources for provisioning a service (Figure 1).

Figure 1. Abstracted Network Resources Defined in Cisco Secure Network Container



This approach optimizes a finite set of logical resources – such as virtual LAN (VLAN), virtual routing and forwarding (VRF), firewall, load balancers, Cisco Wide Area Application Services (WAAS), virtual context, and subnet management – and offers the capability to reuse these resources on each virtual machine that is placed in the same container.

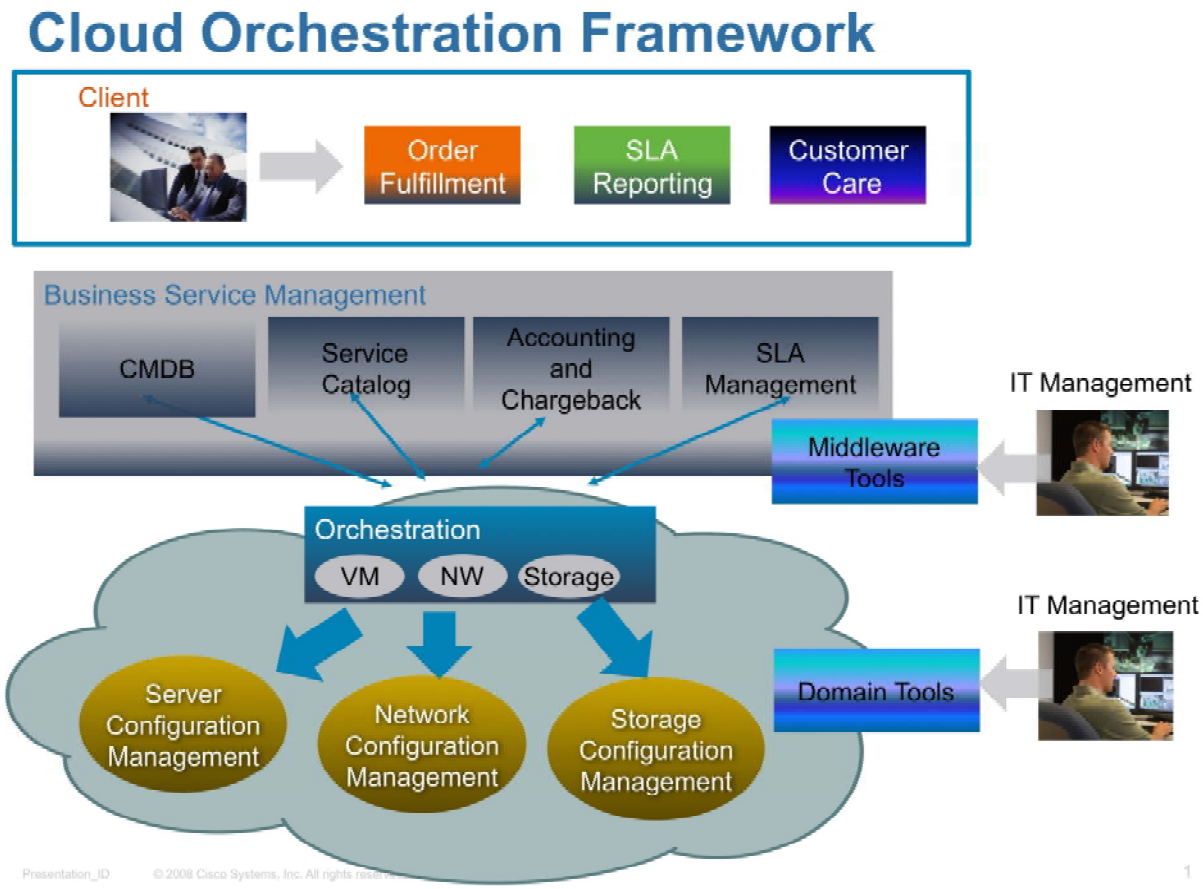
Cisco Secure Network Container offers the following advantages:

- Manages the interdependencies of resources, helping ensure that Layer 2 through 7 connectivity works logically and can match physically the design of the network topology
- Spans the entire network, from a Multiprotocol Label Switching (MPLS) routed core network coming in from an IP Next-Generation Network (IP NGN) to the server access switch layer, including all the firewall and load-balancing services at the distribution layer
- Integrates with each virtual machine being added through a portal through the mapping of virtual network interface cards (NICs) and port groups to the container names, which in turn are mapped to the underlying access VLANs and other settings at the virtualized server and network layers
- Allows secure, compliant segregation of virtual and physical resources per tenant
- Enables interoperability of industry-standard services (such as VLANs and VPNs) across providers and infrastructure

Cisco Secure Network Container in a Service Orchestration Framework

A service orchestrator allows application administrators to define and automate a set of tasks (such as tasks related to configuration view, catalogs, and service-level agreements [SLAs]) and then specify rules and coordinate these tasks across networking, computing, and storage infrastructure. Cisco Secure Network Container can be used together with a service orchestration tool or management framework to supply the network-related linkages, helping enable a unified structure and network services upon which the orchestration engine can dynamically provision applications in the cloud (Figure 2).

Figure 2. Cloud Service Orchestration Framework



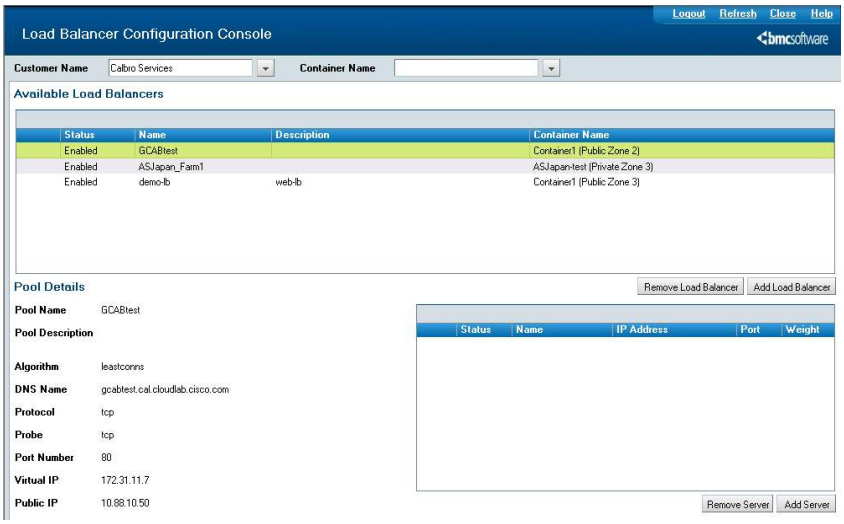
In Figure 2, the top layer portrays what the customer sees through a self-service portal that is enabled with a service orchestration framework solution. Below this, business service management features may include a configuration management database (CMDB), specific application software from a service catalog, an accounting and chargeback application, and SLA management software. The service orchestrator then orchestrates end-user service requests back and forth from resources that may include virtual and physical computing, networking, and storage infrastructure. Cisco Secure Network Container abstracts and consolidates network configurations related to a particular service.

Main Benefits of Cisco Secure Network Container

Two significant operational benefits that service providers can achieve with Cisco Secure Network Container are mass provisioning of separate customers or data center tenant resources and efficient mapping of interdependent cloud services.

- **Mass provisioning:** Traditionally, addition of resources for a new tenant has required the coordination of network services among various teams to configure those services. On average, 200 to 300 command lines per tenant are needed, requiring a very time-consuming process (300 command lines for device configuration multiplied by 100 tenants, for example, results in 30,000 command lines). Using automated network containers that encapsulate various service catalogs, however, a network administrator can provision a new tenant and configure the required services across the network in minutes. The container approach enables the efficient and automated scaling of hundreds of tenants and thousands of virtual machines with just a few simple steps. Figure 3 is an example of a Cisco Secure Network Container template for configuration of load balancers as part of a new cloud service.

Figure 3. Cisco Secure Network Container Configuration Template for Load Balancers



- **More efficient mapping:** The complex, interdependent mappings and parameters of a container are stored in a CMDB, eliminating the need for a network administrator to maintain such information in a separate silo. With these mappings stored in a configuration database, fewer opportunities exist for errors because the entire process is automated. In addition, the information is more consistent and is readily available across the entire organization. Automated mapping also helps ensure that resources, services, and security do not conflict or become incorrectly configured: problems that can result in orphan virtual machines (where excess capacity is not being used), broken communication paths, or cross-connects between tenants across the network topology.

Integration with Ecosystem of Cloud Service Tools

Cisco Secure Network Container is designed for use by a broad ecosystem of cloud orchestration and service catalog vendors. Beneath the network container abstraction are device-level command-line interfaces to XML-based abstractions of each service component for multiple platforms and topology designs that ecosystem partners can incorporate into their solutions. These device-level interfaces become part of the workflow that is understood by a high-level orchestration engine. The workflow includes variables associated with a container, and the orchestration engine inserts the available resources while maintaining the tenant context. A workflow can include multiple device types, but in most scenarios it uses a specific device category. Examples of variables include IP addresses, a customer's unique variables, virtual services such as security and load balancing, and context IDs. Cisco Secure Network Container templates can also be reused across multiple tenants.

These template-based service components have been validated in large-scale test environments at Cisco, in which automation of the processes of adding customers and hosting virtual machine configurations has been replicated.

Cisco service provider customers can confidently expect production-quality implementations based on architectures consistent with tested standards such as the Cisco Virtual Machine Data Center Reference Design.

Abstracting and Automating Service Tiers

Because each Cisco Secure Network Container can encapsulate and abstract many of the device-level networking components and technologies that enable services, the solution also makes it easier to provision and promote differentiated service tiers for customers. In Figure 4, different service attributes for Gold, Silver, and Bronze service tiers include features such as VRF, VLANs, server load balancing (SLB), and SSL.

Figure 4. Service Tiers Defined by Cisco Secure Network Container

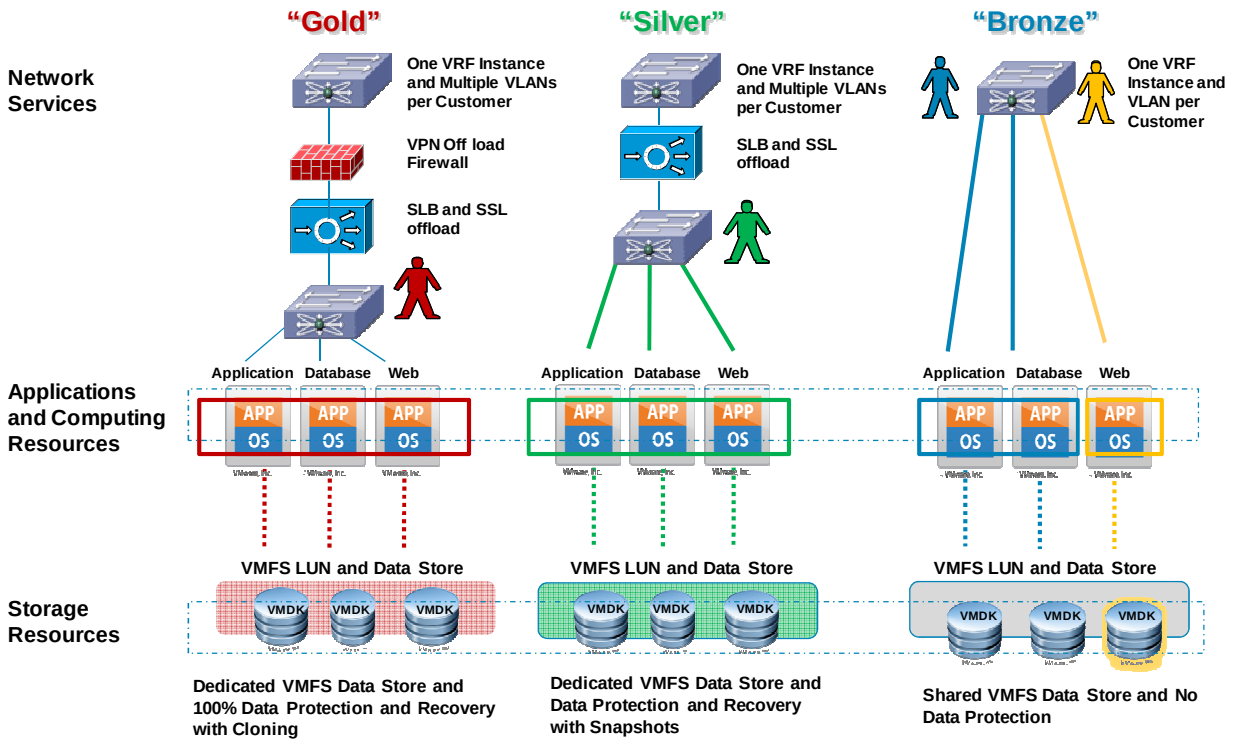


Table 1 shows the differentiated services defined in Cisco Network Service Containers for each service tier.

Table 1. Service Tier Attributes Defined in Cisco Secure Network Containers

Service Attribute	Gold Tier	Silver Tier	Bronze Tier
Ratio of virtual machines to physical machines	1:1	2:1	4:1
Bandwidth reserved	40%	30%	20%
Network components	VLAN, VRF, firewall, and SLB	VLAN, VRF, and SLB	VLAN and VRF
Disaster recovery	Yes	Yes	No
Backup retention	1 month, 6 months, and 1 year	1 month, 6 months, and 1 year	None

On the basis of the customer's choice of service tier, the appropriate workflow will be coordinated by the service orchestration tool. Lower-level processing is initiated with jobs created in the network configuration layer.

Why Cisco

Cisco understands the requirements for scalable, secure cloud computing and has led the industry in building highly scalable networks of all kinds across multiple lines of business and in multiple customer and service provider environments. Now Cisco is aggressively engineering its switching, routing, server, firewall, load-balancing, and

other platforms to make them ready for cloud services. In addition to providing best practices for design, deployment, and operation within the cloud infrastructure, Cisco is an authority on virtual machine scalability, security, mobility, high availability, and optimization.

The result is a next-generation cloud computing platform for the data center that unites computing, networking, storage, and virtualization into one cohesive system. To validate such a set of computing resources, Cisco has invested in large-scale cloud-centric labs in which server, networking, storage, and hypervisor technologies are integrated and tested for the deployment of multi-tenant cloud services.

Cisco understands the challenges of provisioning services as part of abstracted, fully automated provisioning systems and is working with a range of ecosystem partners that are providing cloud service, portal, and orchestration layers that rely on the integration of well-defined network services.

Conclusion

Cisco Secure Network Container is a powerful new solution for encapsulating various shared resources that are abstracted to provide a fast, simplified method for provisioning and automating cloud services. With Cisco Secure Network Container, network resources can be quickly configured to offer differentiated services, providing application flexibility and customer choice. To the service provider, Cisco Secure Network Container offers a centralized view and configuration control of network resources, enabling exceptional ease of provisioning, automation, and change management. Cisco's ecosystem partners can integrate with Cisco Secure Network Container using a high-level orchestration engine that allows cloud service providers to provision robust cloud services in minutes instead of days.

For More Information

Cisco Unified Service Delivery: http://www.cisco.com/go/usd

Cisco Service Provider Data Center: http://www.cisco.com/go/spdatacenter

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 C11-636984-00 11/10