



Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform – Tenant Portal Guide, Release 2.1

October 12, 2016

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE 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 THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Service Provider Segment

Cloud and Network Solutions

Cisco Cloud Architecture for the Microsoft Cloud Platform Solution

Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 2.1

Part: CCAMCP-CNAP-Tenant2-2.1

© 2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

Document Objective and Scope 2-v

CHAPTER 1

Introduction 1-1

Tasks You Can Perform in the Tenant Portal 1-1

Understanding the Interrelationship of Tasks Performed in the Tenant Portal and by the Cloud Provider 1-2

Accessing the Tenant Portal 1-2

Subscribing to a Plan 1-4

Creating a Container 1-9

CHAPTER 2

Viewing and Modifying Information about Containers 2-1

Viewing Summary Information about a Container 2-2

Deleting a Container 2-6

Viewing Gateway Information about a Container 2-8

Setting up an Internet WAN Gateway 2-10

Setting up a Site-to-Site VPN 2-19

Removing a MPLS WAN Gateway 2-21

Viewing and Modifying Firewall Information about a Container 2-21

Understanding Firewall Creation 2-22

Viewing Summary Information about a Firewall 2-22

Viewing the Hierarchy of Information on the Firewall Tab 2-24

Configuring a Firewall 2-28

Changing a Policy Map for a Service Policy 2-31

Adding a New Class Map 2-32

Changing a Class Map 2-35

Creating a New Network Access Control List 2-36

Changing an Access List 2-39

Creating a New Object Group 2-40

Changing an Object Group 2-45

Viewing and Modifying Tier Information about a Container 2-48

Adding a Tier 2-50

Adding a Segment 2-51

Changing a Tier 2-51

Updating a Segment 2-52
Removing a Tier 2-53
Mapping Public IP Addresses to Private DMZ IP Addresses 2-53

APPENDIX A

Onboarding an Application from a Subscription A-1



Preface

This document describes how to use the Tenant Portal of the Cisco Cloud Network Automation Provisioner (CNAP) for the Microsoft Cloud Platform (MCP).

Document Objective and Scope

This document is part of the Cisco Cloud Architecture for the Microsoft Cloud Platform (CCA MCP) documentation suite for Release 1, summarized in the following table.

Table 2-1 CCA MCP Documentation Suite

Document	Description
Release Notes for Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 2.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-RNs/CNAP2-Release-Notes.html	Describes caveats and other important information about Release 2.1.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 2.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/Foundation/CCAMCP1_Foundation.html	Describes data center infrastructure setup and implementation to support CCA MCP based services.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Zinc Container Configuration Guide, Release 2.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/IaaS_Zinc_Config/CCAMCP1_IaaS_Zinc_Config.html	Describes the Infrastructure as a Service (IaaS) model with per-tenant Cisco CSR 1000V-based router/firewall.

Table 2-1 CCA MCP Documentation Suite

<p>Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 2.1</p> <p>http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-Install/CNAP2-Install.html</p>	<p>Describes the procedures and initial configuration to install Cisco CNAP in a data center.</p>
<p>Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Admin Portal Guide, Release 2.1</p> <p>http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-Admin/CNAP2-Admin.html</p>	<p>Describes how the Cisco CNAP Admin Portal is used to create and manage network container plans.</p>
<p>Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 2.1</p> <p>http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-Tenant/CNAP2-Tenant.html</p>	<p>Describes how the Cisco CNAP Tenant Portal is used to subscribe to network container plans and manage subscriptions.</p>
<p>Cisco Cloud Architecture for the Microsoft Cloud Platform: DBaaS Configuration Guide, Release 1.0</p> <p>http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/DBSQLaaS/CCAMCP1_DBaaS.html</p>	<p>Describes how Database as a Service (DBaaS) can be deployed over the CCA MCP solution.</p>
<p>Cisco Cloud Architecture for the Microsoft Cloud Platform: DRaaS Application Note, Release 1.0</p> <p>http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/DRaaS_Application_Note/DRaaS_ASR.html</p>	<p>Describes how Disaster Recovery as a Service (DRaaS) based on Microsoft Azure Site Recovery can be deployed over the CCA MCP architecture.</p>
<p>Cisco Cloud Architecture for the Microsoft Cloud Platform: Backup as a Service Implementation Guide, Release 1.0</p> <p>http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/BaaS/BaaS_CommVault.html</p>	<p>Describes how Backup as a Service (BaaS) based on Commvault Simpana software can be deployed over the CCA MCP architecture.</p>

This document only describes the Cisco CNAP Tenant Portal. For information on using the Admin Portal of the Cisco CNAP for MCP, see the Admin Portal Guide listed in the table above.



CHAPTER 1

Introduction

The Cisco Cloud Architecture for Microsoft Cloud Platform (CCA for MCP) solution delivers IaaS, PaaS, and SaaS with integrated management software. The data center infrastructure is built with Cisco Application Centric Infrastructure (ACI) for the Data Center Fabric and Cisco UCS-based compute, Cisco Adaptive Security Appliance (ASA) firewall for security, and Cisco Aggregation Services Routers (Cisco ASR 9000 and Cisco ASR1000) data center edge routers. Additionally, Cisco virtualized network functions such as Cisco Cloud Services Router 1000V (CSR 1000V) are used to implement tenant services.

Microsoft Hyper-V Hypervisor is used as the virtualizing layer for compute to run tenant workloads. The Management Stack is based on Microsoft Windows Azure Pack (WAP), which allows service providers to create plans and tenant administrators to subscribe to those plans.

CCA for MCP enables service providers to offer network management services on top of a Cisco network infrastructure through Microsoft WAP. A Microsoft WAP administrator can use the Cisco Cloud Network Automation Provisioner (CNAP) for MCP Admin Portal to configure, manage, and administer Cisco Data Center Network resources. Cisco CNAP provides the capability to create tenant containers with sophisticated network services such as tenant edge routing, multiple security zones, firewalling, NAT, MPLS VPN access, and Server Load Balancing. The administrator uses the portal to define and set up the available plans that will be visible in the Tenant Portal and that can be consumed by tenants. Tenants consume resources by using the Tenant Portal to subscribe to an available plan. This allows service providers to offer differentiated plans that provide more value to tenants and generate more revenue for service providers, with the convenience of automation to deploy sophisticated containers for tenants.

For more information, see: <http://www.cisco.com/go/cloud>.

Tasks You Can Perform in the Tenant Portal

You can use the Tenant Portal to:

- Subscribe to plans
- Create containers for subscriptions

In a multi-CSR container plan, multiple “subcontainers” are logically stitched together by Cisco CNAP to form one “super container”. A multi-CSR container plan lets you scale out your network performance through the provisioning of additional Cisco CSR 1000V routers, allocate Cisco CSR 1000Vs and the associated workload subnets to specific applications, and allocate Cisco CSR 1000Vs according to departments or work groups within your organization.

- View and modify information about containers, including:

- View summary information about a container.
- Delete a container.
- View gateway information about a container, including remove a WAN gateway.
- View and modify firewall information about a container, including add and modify a policy map for a service policy, modify and remove a class map instance, and modify and remove an access group (you can also add a rule to an Access Control List [ACL]).
- View and modify tier information about a container, including add a tier, change a tier (and update a segment), remove a tier, and remove a segment.
- Map public IP addresses to private DMZ IP addresses

Understanding the Interrelationship of Tasks Performed in the Tenant Portal and by the Cloud Provider

Certain tasks performed in the Tenant Portal and by the cloud provider are interdependent in that tasks must be completed by one user before other tasks can be accomplished by the other user. For example:

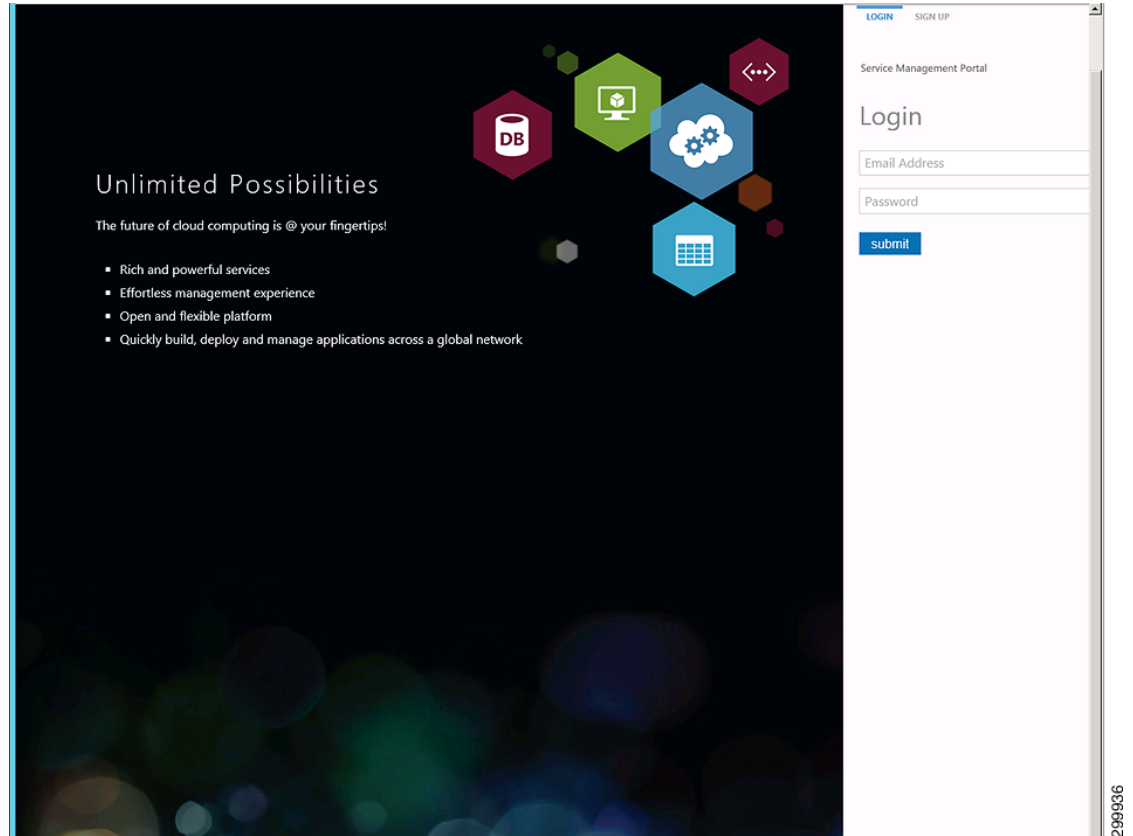
- Base container plans must be created by the cloud provider before you can use the Tenant Portal to subscribe to them and create containers.
- In the Tenant Portal, after you subscribe to a plan and create a container, then the cloud provider can confirm that the newly-created tenant container is Active and configure the following for it:
 - WAN Gateway—When you are creating a container for a plan to which you have subscribed, you see a screen indicating whether the plan includes entitlement for a WAN Gateway (e.g., MPLS VPN). If it does, you see a message to contact your cloud provider. Once your container is active, the cloud provider can then configure the WAN Gateway.
 - Firewall—When you are creating a container for a plan to which you have subscribed, you specify the number of Workload Tiers for the container. Cisco CNAP will automatically set up a perimeter around each of the zones in the container, however the Tenant Firewall tab will not display any information until the WAN Gateway has been provisioned by the cloud provider. The firewall is automatically created with a base configuration during container creation. When the WAN gateway is created, another firewall zone is created for the WAN edge. You can configure a firewall in the Tenant Portal, however it can only be configured after you have created a container and the cloud provider has created a WAN Gateway.

Accessing the Tenant Portal

You access the Tenant Portal from the WAP Tenant Site.

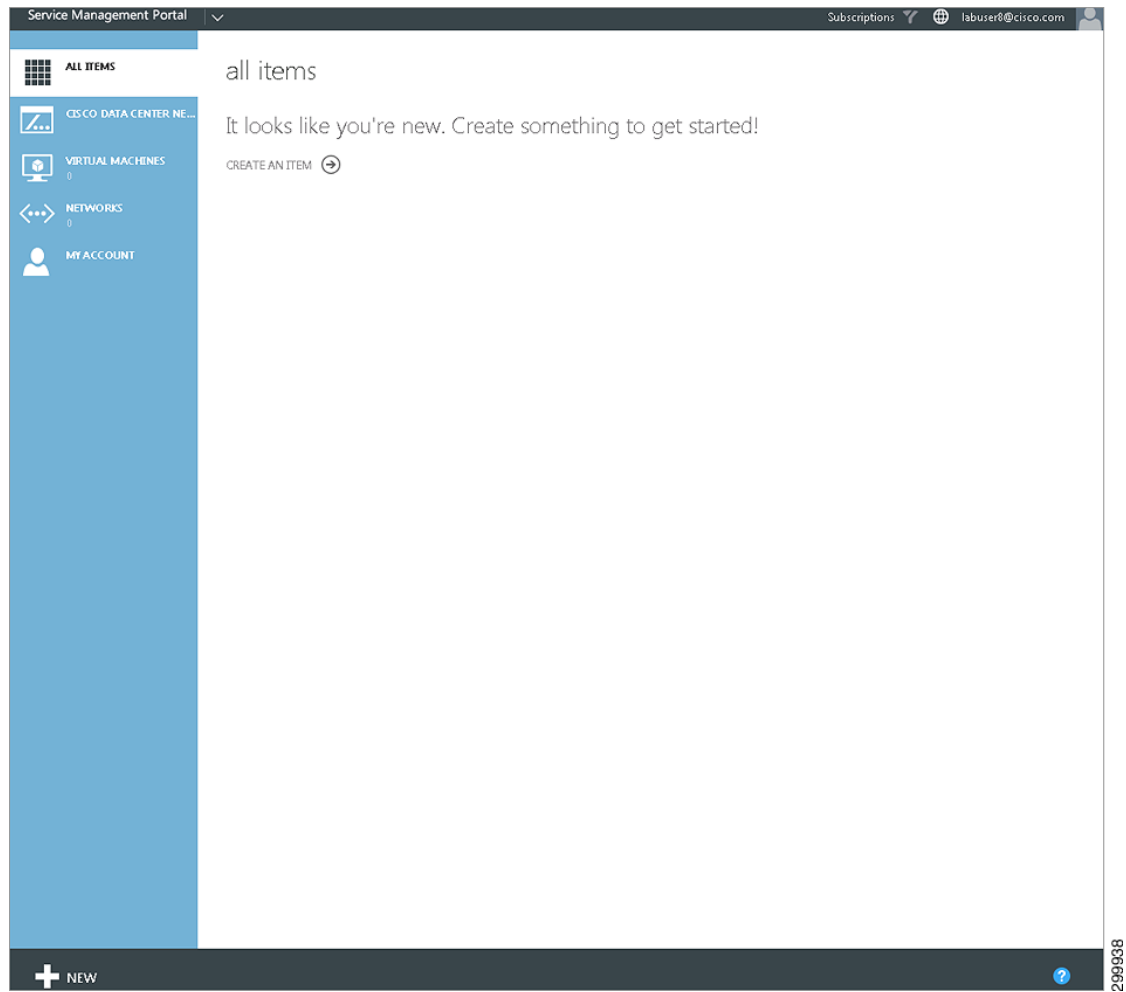
To access the Tenant Portal:

-
- Step 1** Access WAP.
For information on accessing WAP, see the WAP documentation.
 - Step 2** You see the WAP Tenant Portal login screen, shown in the following screen.

Figure 1-1 WAP Tenant Portal Login Screen

- Step 3** Enter your login credentials (email address and password) and click **submit**. You see the main Tenant Portal screen, shown in the following screen.

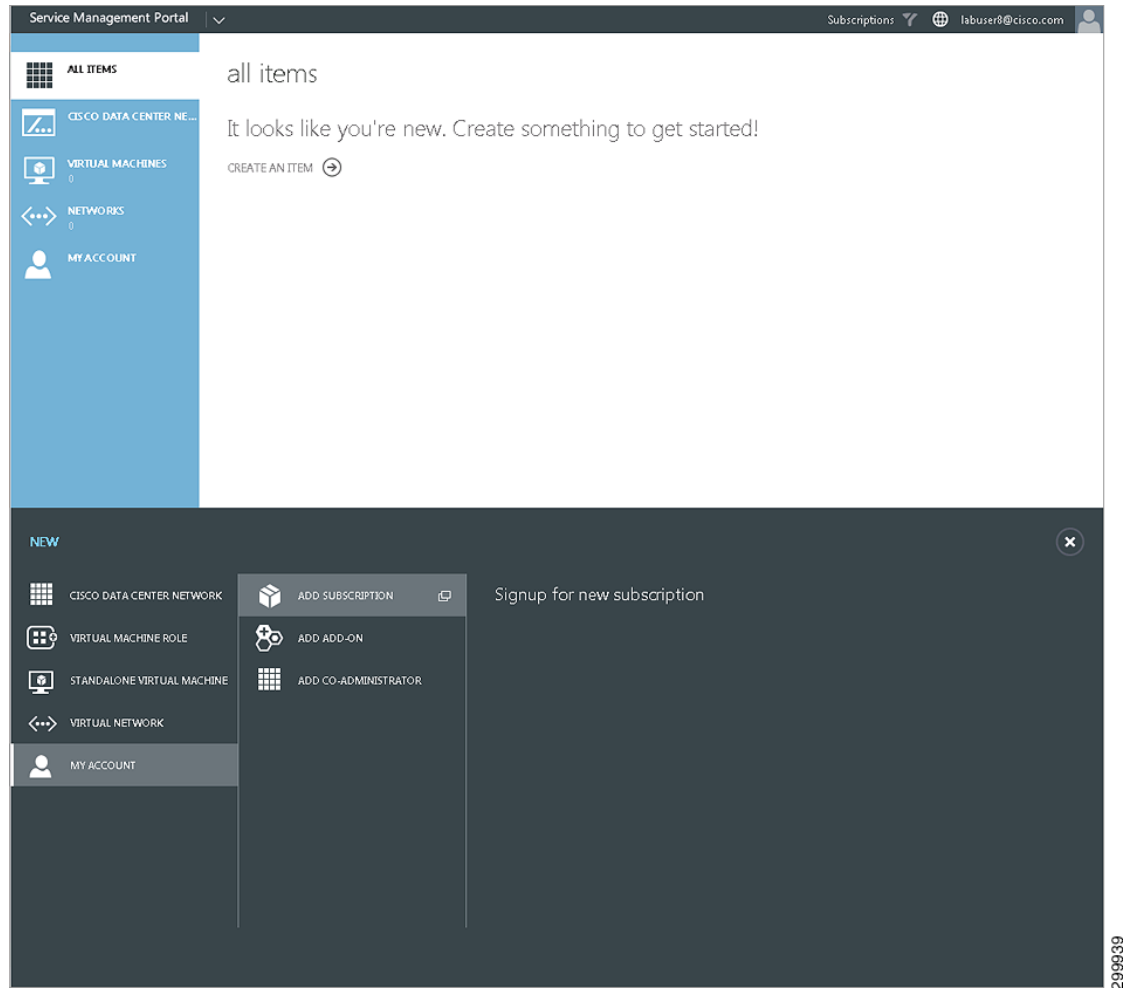
Figure 1-2 Main Tenant Portal Screen



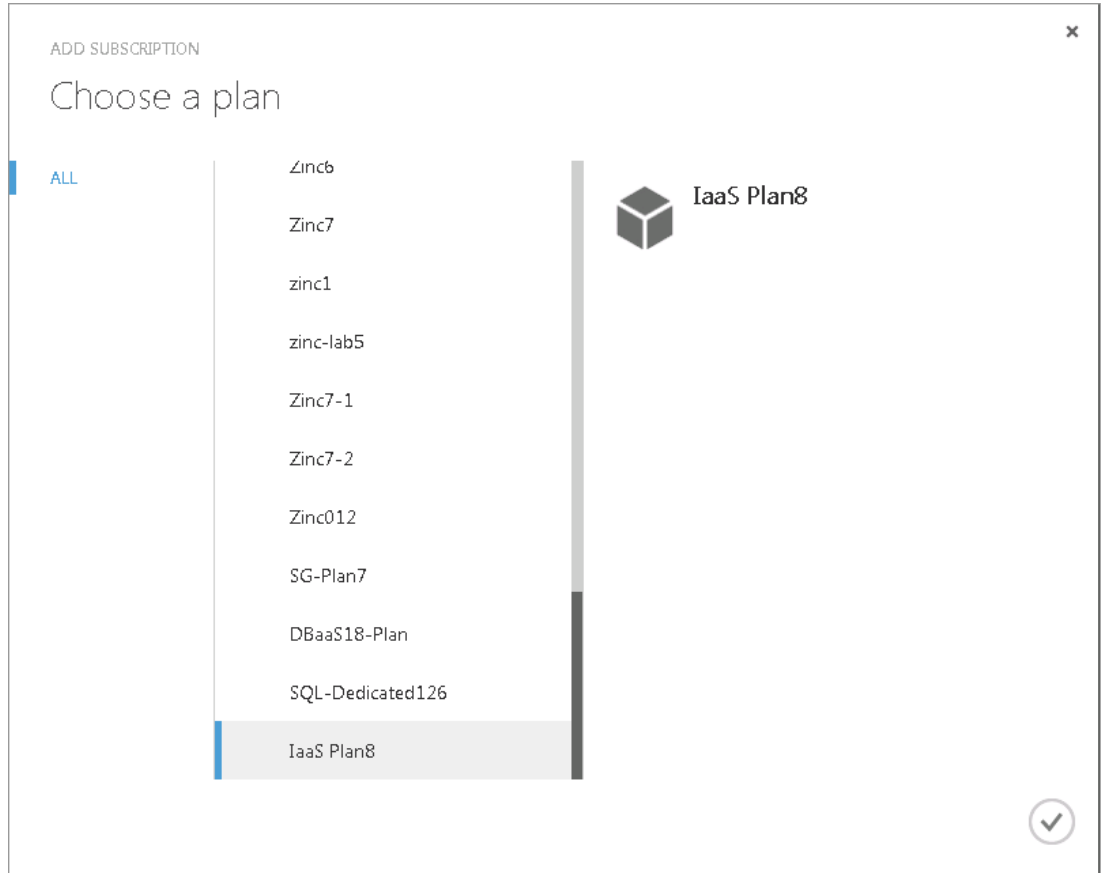
Subscribing to a Plan

To subscribe to a plan:

- Step 1** On the main Tenant Portal screen, at the bottom, click **+ New** in the lower left corner, click **My Account**, then click **Add Subscription**, as shown in the following screen.

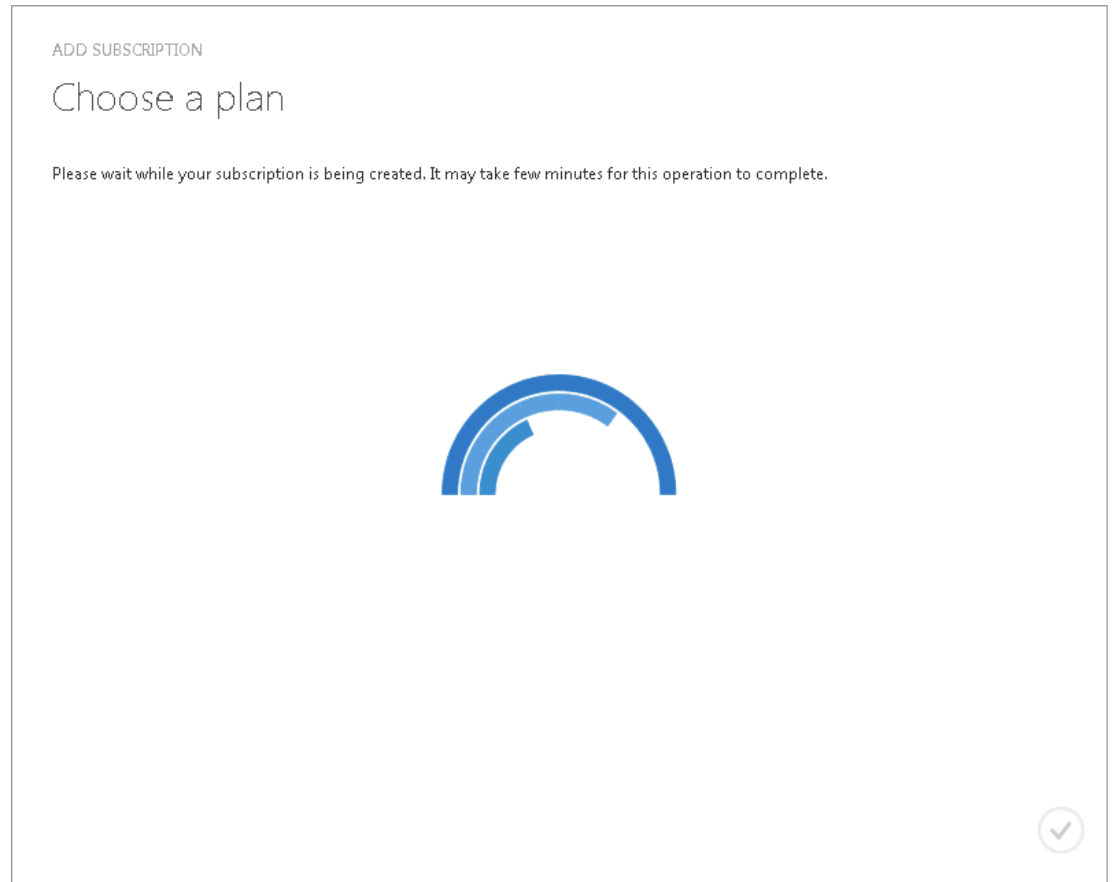
Figure 1-3 Add Subscription Screen

You see the Choose a Plan screen, as shown in the following screen.

Figure 1-4 Choose a Plan Screen

- Step 2** Click the plan to which you want to subscribe (in this example **IaaS Plan8**), then click the check mark. You see the following screen while the subscription is being created.

Figure 1-5 Subscription Being Created Screen



Next you see a screen showing the plan to which you subscribed with a Status of Syncing, as shown in the following screen.

Figure 1-6 Plan Subscription Syncing

my account

SUBSCRIPTIONS ADD-ONS MANAGEMENT CERTIFICATES ADMINISTRATORS

SUBSCRIPTION ID	SUBSCRIPTION	STATUS	PLAN	ENROLLMENT DATE
2825839c-d18a-45b8-a8e5...	Zinc8	Active	Zinc8	9/22/2015 3:58:38 PM
dd64abab-700d-4b31-ac98-705...	IaaS Plan8	Active	IaaS Plan8	9/25/2015 2:00:22 PM
8f446d51-44b0-469c-8e5e-f36b...	Test Plan 8	Active	Test Plan 8	9/25/2015 3:13:15 PM
d5be44a2-d310-4b11-aa1c-df0c...	Zinc7	Active	Zinc7	9/25/2015 3:27:45 PM
abb3ea00-85a8-4482-b09c-540...	IaaS Plan3	** Syncing	IaaS Plan3	9/28/2015 11:03:15 AM

NEW DELETE CHANGE NAME

299942

When the synchronization is complete, the subscription will show as Active, as shown in the following screen.

Figure 1-7 Plan Subscription Active

SUBSCRIPTION ID	SUBSCRIPTION	STATUS	PLAN	ENROLLMENT DATE
2625938c-d18a-45b8-abe5-ee...	Zinc8	Active	Zinc8	9/22/2015 3:50:38 PM
dd64abab-700d-4b31-ac98-705...	IaaS Plan8	Active	IaaS Plan8	9/25/2015 2:00:22 PM
8f446d51-4460-466c-8e5e-f36b...	Test Plan 8	Active	Test Plan 8	9/25/2015 3:13:15 PM
d5be44a2-d310-4b11-aa1c-ct0c...	Zinc7	Active	Zinc7	9/25/2015 3:27:45 PM
abb3ea00-85a8-4482-b09c...	IaaS Plan3	Active	IaaS Plan3	9/28/2015 11:03:15 AM

Creating a Container

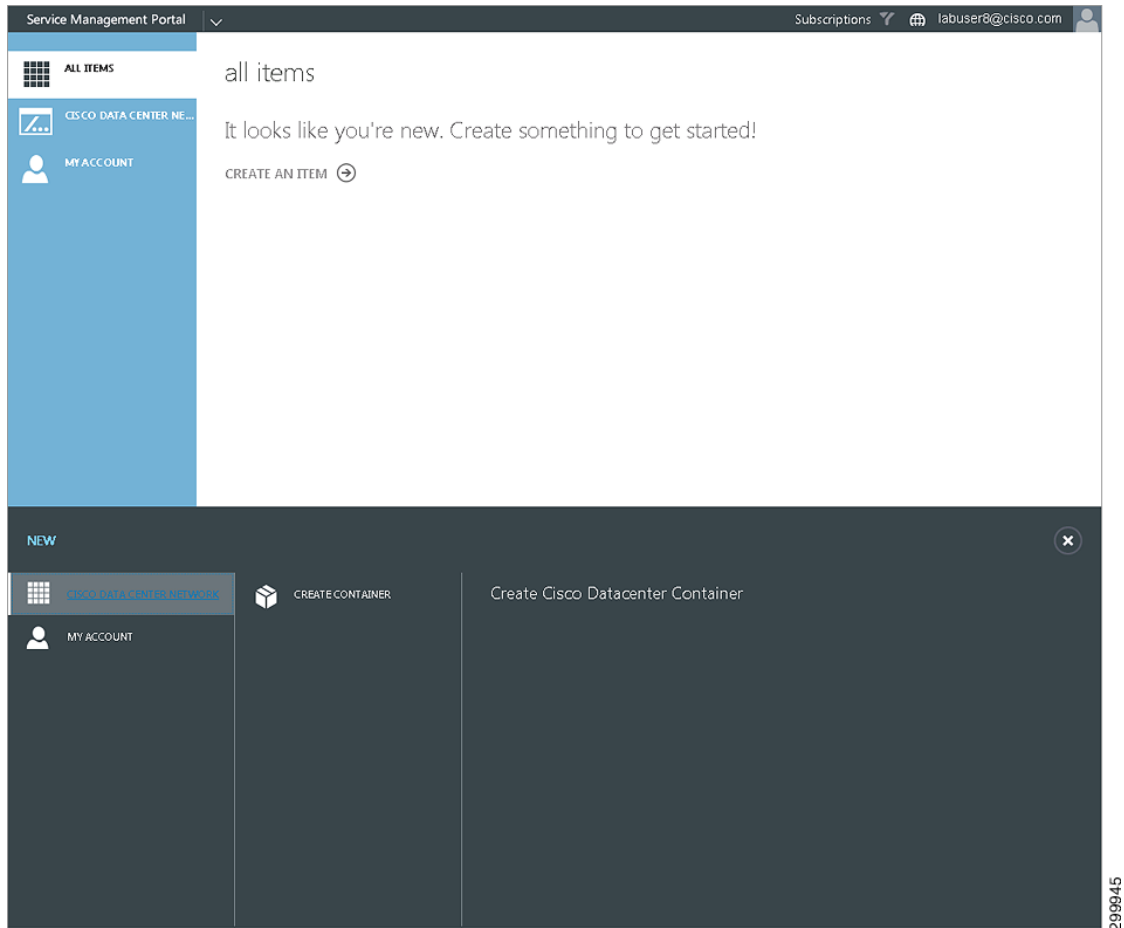


Note

You use Cisco CNAP to create network containers. **After** you create a container, use the VM cloud resource provider (RP) to allocate VMs to the tiers in a container. Standalone mode will always work and should generally be used unless your SP gives you other instructions. VM roles mode will only work if your SP is using addresses from a static IP address pool. Contact your SP to determine which mode you should use.

To create a container:

- Step 1** On the main Tenant Portal screen, click **+ New** in the lower left corner, then click **Cisco Network**, then **Create Container**, as shown in the following screen.

Figure 1-8 Create New Container Screen

You see the following screen.

Figure 1-9 Container Creation Screen

Cisco Datacenter Network Container ✖

Subscription

Plan Name :

Admin:

Regions :

Container Details

Name :

Type :

Bring Your Own IP Space Multi CSR

Container Group : ✕

WAN Access

MPLS VPN Site-To-Site VPN Remote VPN

Internet Access Autoprovision WAN Edge/PE

Tiers

Workload :

Workload SLB

DMZ :

DMZ SLB

Shared Services :

Cancel

Next ➤

Step 2 Some values are prepopulated based on what your cloud provider has defined. Complete the fields to create a network container:

- Subscription:
 - Subscription:—Select the subscription for which you want to create a container.
 - Admin:—Preselected and cannot be changed.
 - Regions:—Select the Region with which the container will be associated.
- Container Details:
 - Name:—Enter a name for the container or use the prepopulated name.
 - Type:—**Zinc Container** is supported in the current release.
 - Bring Your Own IP Space (BYoIP)—BYoIP allows you to assign your own preferred address space (subnet) to each of the Workload Tiers within your conjoined container. To prevent conflicts, you must assign a unique, non-overlapping subnet to each of the Workload Tiers during container creation. This allows your Enterprise users access to the Workload Virtual Machines and Load Balancers (if applicable) as part of your Enterprise Network.



Note

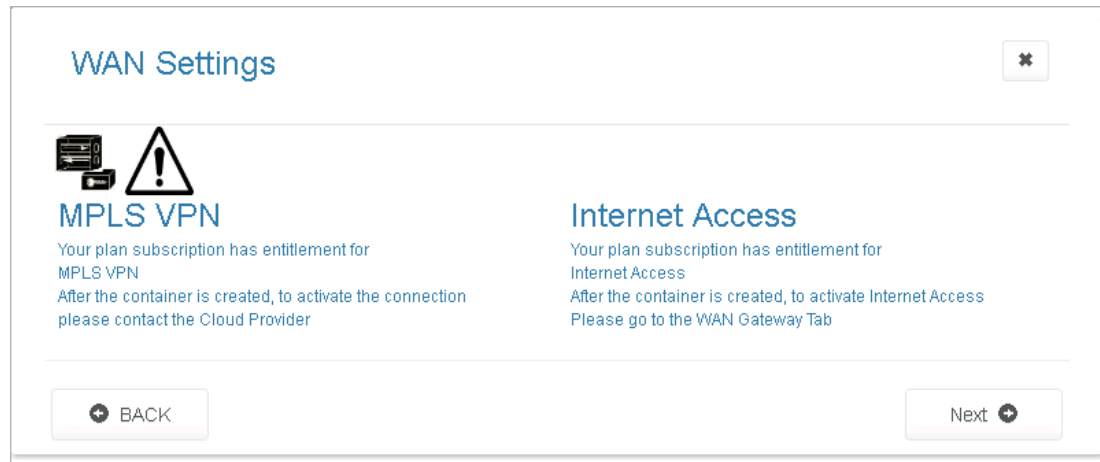
When Multi-CSR is checked, BYoIP is **required** but the Bring Your Own IP Space checkbox is not selected. When Multi-CSR is not selected, BYoIP is **not** supported.

- Multi CSR—If this is checked, then you can scale out your network performance through the provisioning of additional Cisco CSR 1000V routers, allocate Cisco CSR 1000Vs and the associated workload subnets to specific applications, and allocate Cisco CSR 1000Vs according to departments or work groups within your organization.
- Container Group—Container groups are optional descriptors you can add at container creation. In the event that master containers are being used (multiCSR), using the same container group for multiple containers keeps them in the same master container. If multiple master containers are not required, the field can be ignored.
- WAN Access (VPN):
 - MPLS, Site-to-Site, and Internet are supported in the current release. Remote Access is not supported.
- Tiers:
 - Workload:—Number of tiers.
 - Workload SLB—Preselected based on plan.
 - DMZ:—DMZ tier for external (Internet) access.
 - DMZ SLB—DMZ server load balancer.

When you are finished, at the bottom of the screen, click the right arrow (→).

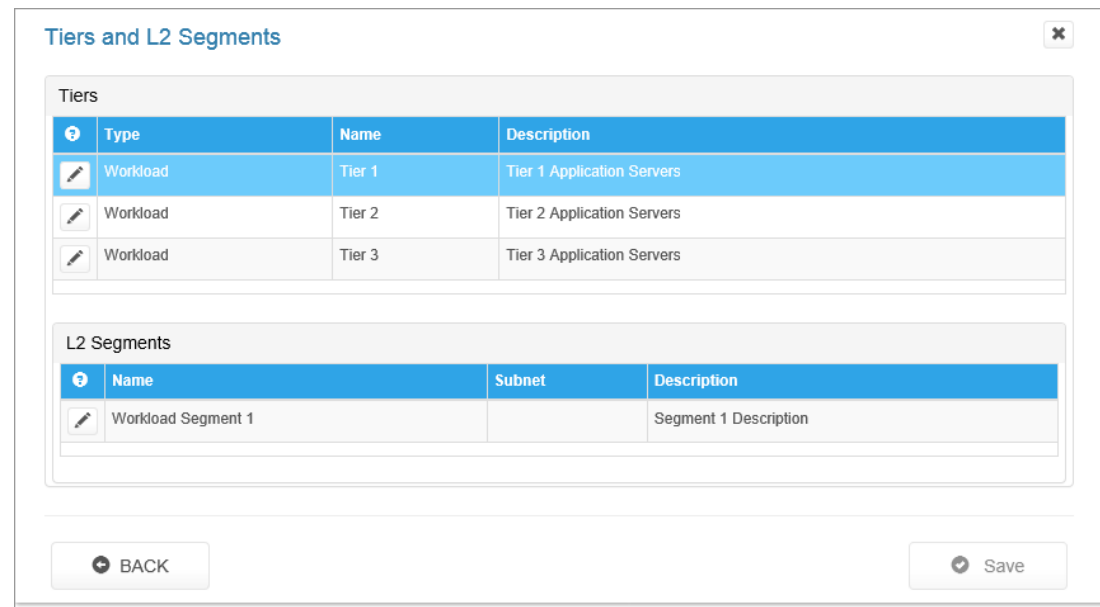
You see the following screen if the plan is entitled to an MPLS VPN and Internet Access. If the plan is only entitled to an MPLS VPN, you do not see the message about Internet Access.

Figure 1-10 WAN Gateway and Internet Access Screen



- Step 3** Click the right arrow (→).
You see the following screen.

Figure 1-11 Tiers and Layer 2 Segments Screen



On the Container Creation screen we specified three (3) Workload Tiers and one (1) DMZ Tier under Tiers, so this screen shows those structures already created.

This screen displays the following information:

- Tiers:
 - Type—Workload and DMZ are supported in this release.
 - Name—Name of the tier.
 - Description—Description of the tier.
- L2 Segments:

- Name—Name of the segment.
- Subnet—Subnet the segment is in. The next step details the procedure for entering subnet information for a multi-CSR container.
- Description—Description of the segment.

Step 4 In a multi-CSR container, for each Tier, you need to enter the subnet information for the Tier segment. Click the Tier you want to update to highlight it, then click the pencil icon next to the corresponding segment under L2 Segments.

You see the following screen.

Figure 1-12 Change Segment Screen

Step 5 Enter the subnet information for the segment. You can use /24 to /29 masks for workload tier subnet IP addresses. When you are finished, click **Update**.

You return to the previous screen.

Step 6 Select each remaining Tier in turn and enter the subnet information for its segment. When you are finished, click **Save**.



Note

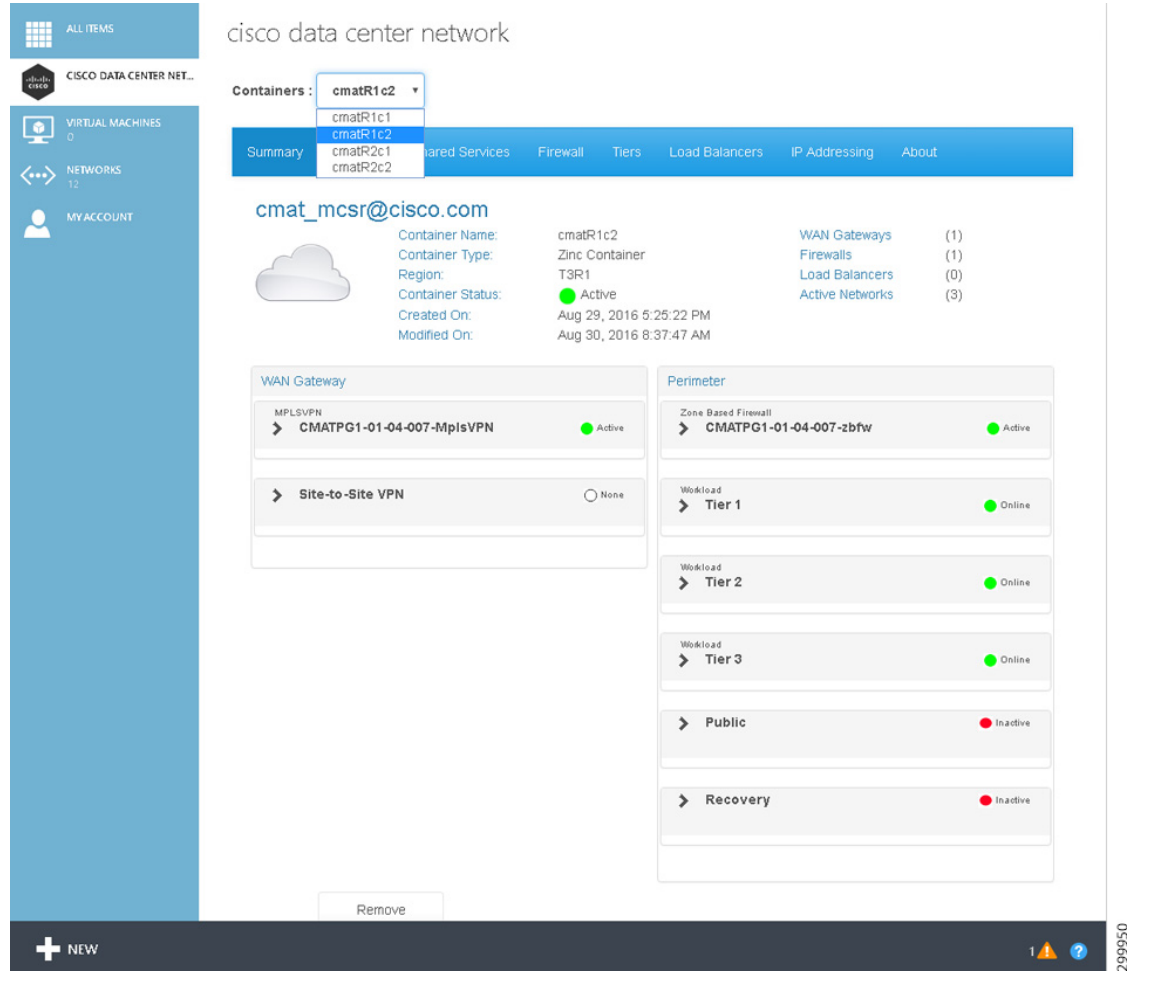
In a multi-CSR container, you must select each region in turn from the drop-down menu on the Container Creation Screen shown in [Figure 1-9](#) and update the subnet information for the tier segments in that region following the procedure above.

Step 7 When you are finished, click the check mark.

Step 8 Click **Cisco Network**.

The container you created should be available in the Containers: pull-down menu at the top of the screen, as shown in the following screen.

Figure 1-13 Container Pull-down Menu Screen





CHAPTER 2

Viewing and Modifying Information about Containers

You can view and modify a variety of information about containers, including:

- View summary information about a container
- Delete a container
- View gateway information about a container, including:
 - Set up an Internet WAN gateway for Internet access
 - Set up a Site-to-Site gateway
 - Remove a MPLS WAN gateway
- View and modify firewall information about a container, including:
 - View summary information about a firewall
 - View the hierarchy of information on the Firewall tab
 - Configure a firewall
 - Change the policy map for a service policy
 - Add a new class map
 - Change a class map
 - Create a new network Access Control List (ACL)
 - Change an Access Control List
 - Create a new object group
 - Change an object group
- View and modify tier information about a container, including:
 - Add a tier
 - Change a tier (and update a segment)
 - Remove a tier
 - Remove a segment
- Map public IP addresses to private DMZ IP addresses

Viewing Summary Information about a Container

- Step 1** To display summary information about a specific container instance, click **Cisco Network**. You see the Tenant Summary Tab screen.

Figure 2-1 Tenant Summary Tab Screen

The screenshot shows the 'Tenant Summary Tab Screen' for a container named 'cmatR1c2'. The interface includes a navigation sidebar on the left with sections for 'ALL ITEMS', 'CISCO DATA CENTER NET...', 'VIRTUAL MACHINES', 'NETWORKS', and 'MY ACCOUNT'. The main content area is titled 'cisco data center network' and features a 'Containers' dropdown menu with options: 'cmatR1c2', 'cmatR1c1', 'cmatR2c1', and 'cmatR2c2'. Below the dropdown is a horizontal menu with tabs: 'Summary', 'Shared Services', 'Firewall', 'Tiers', 'Load Balancers', 'IP Addressing', and 'About'. The 'Summary' tab is active, displaying details for 'cmat_mcsr@cisco.com'. The details include: Container Name: cmatR1c2, Container Type: Zinc Container, Region: T3R1, Container Status: Active (indicated by a green dot), Created On: Aug 29, 2016 5:25:22 PM, and Modified On: Aug 30, 2016 8:37:47 AM. To the right of these details is a summary table:

WAN Gateways	(1)
Firewalls	(1)
Load Balancers	(0)
Active Networks	(3)

Below the details are two main sections: 'WAN Gateway' and 'Perimeter'. The 'WAN Gateway' section contains a table with two rows:

MPLSVPN	CMATPG1-01-04-007-MpisVPN	Active
Site-to-Site VPN		None

The 'Perimeter' section contains a table with five rows:

Zone Based Firewall	CMATPG1-01-04-007-zbfbw	Active
Workload	Tier 1	Online
Workload	Tier 2	Online
Workload	Tier 3	Online
Public		Inactive
Recovery		Inactive

At the bottom center, there is a 'Remove' button. The bottom of the screen features a dark bar with a '+ NEW' button on the left and a notification icon on the right.

The Tenants Summary screen displays a list of all the WAN Gateway services configured in the container (MPLS VPN, Site-to-Site, Remote Access, and Internet) and a list of all the perimeter network services configured in the container (firewall, tiers, DMZ, etc.).

Specific information above the WAN Gateway and Perimeter tables includes:

- Container Name:—Displays the container name.
- Container Type:—Displays the container type name.
- Region:—Displays the Region name.
- Status:—Displays the container status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
 - Green—Container is Active.

- Red—Container is Inactive.
- Yellow—Container state is Creating.
- Created On:—Displays the date and time when the container was created.
- Modified On:—Displays the date and time when the container was last modified.
- WAN Gateways—Displays the total count of WAN gateways. For example, if MPLS VPN and Site-to-Site were part of the container, the displayed text would be WAN Gateways (2). The icon indicates the status of the WAN Gateway(s): Green, Red, and Gray (icons are only meaningful on initial configuration as status is not routinely monitored).
- Firewalls—Displays the total count of firewalls. For example, if one firewall was part of the container, the displayed text would be Firewalls (1). The icon indicates the status of the firewall(s): Green, Red, and Gray (icons are only meaningful on initial configuration as status is not routinely monitored).
- Load Balancers—Displays the total count of Load Balancers.
- Active Networks—Displays the total count of active networks configured on the container. For example, if there were five total networks, the displayed text would be Active Networks (5).

You can collapse and expand the table information using the triangles, as shown in the following sample screen for the MPLS VPN WAN Gateway and Perimeter Tier 1.

Figure 2-2 Summary Tab—WAN Gateway MPLS VPN Details

The screenshot displays the 'Summary' tab for a container named 'cmatR1c2'. The container is a Zinc Container in the T3R1 region, with a status of 'Active'. It was created on August 29, 2016, at 5:25:22 PM and last modified on August 30, 2016, at 8:37:47 AM. The summary table indicates 1 WAN Gateway, 1 Firewall, 0 Load Balancers, and 3 Active Networks.

The 'WAN Gateway' section shows an active MPLSVPN named 'CMATPG1-01-04-007-MpisVPN'. Its configuration includes:

- Import RT: (blank)
- Export RT: (blank)
- Route Descriptor: 5:522
- VRF: CMATPG1-04
- Primary IP: 10.6.0.71
- Secondary IP: 10.6.0.72
- Mask: 255.255.255.0
- Created On: Aug 30, 2016 8:36:18 AM
- Modified On: Aug 30, 2016 8:37:47 AM

The 'Perimeter' section shows an active Zone Based Firewall named 'CMATPG1-01-04-007-zbfw'. It includes workload tiers (Tier 1, Tier 2, Tier 3) all in an 'Online' state, and 'Public' and 'Recovery' settings both in an 'Inactive' state.

Using MPLS VPN as an example, the information in the WAN Gateway table includes:

- MPLSVPN and name—Gateway type, name of the gateway, and an icon to indicate the status of the VPN (icons are only meaningful on initial configuration as status is not routinely monitored).
- Import RT—The configured RT for the WAN Gateway.
- Export RT—The configured RT for the WAN Gateway.
- Route Descriptor—The configured descriptor based on your cloud provider's network design.
- VRF—Generated by Cisco CNAP based on the abbreviation of the container ID.
- Primary IP—External PE IP Address in dotted format.
- Secondary IP—External PE IP Address in dotted format.
- Mask—External PE Mask in dotted format
- Created On:—Displays the date and time when the WAN Gateway was created.
- Modified On:—Displays the date and time when the WAN Gateway was last modified.

Information in the Perimeter table is based on the currently selected Cloud Service and includes information about firewalls and tiers (in the current release, public for backups and recovery for DMZ are not used).

Figure 2-3 Summary Tab—Perimeter Firewall Details

299952

Using Zone Based Firewall as an example, the information in the Perimeter table includes:

- Zone Based Firewall and name—Firewall type, name of the firewall, and an icon to indicate the status of the firewall (icons are only meaningful on initial configuration as status is not routinely monitored).
- Primary IP—External PE IP Address
- Primary Mask—External PE Mask
- Secondary IP—External PE IP Address
- Secondary Mask—External PE Mask
- Created On:—Displays the date and time when the firewall was created.
- Modified On:—Displays the date and time when the firewall was last modified.

Figure 2-4 Summary Tab—Perimeter Tier Details

299953

Information in the Perimeter table for each Tier includes:

- Seg 1—IP Address of the tier segment.
- Created On:—Displays the date and time when Tier 1 was created.
- Modified On:—Displays the date and time when Tier 1 was last modified.

Deleting a Container



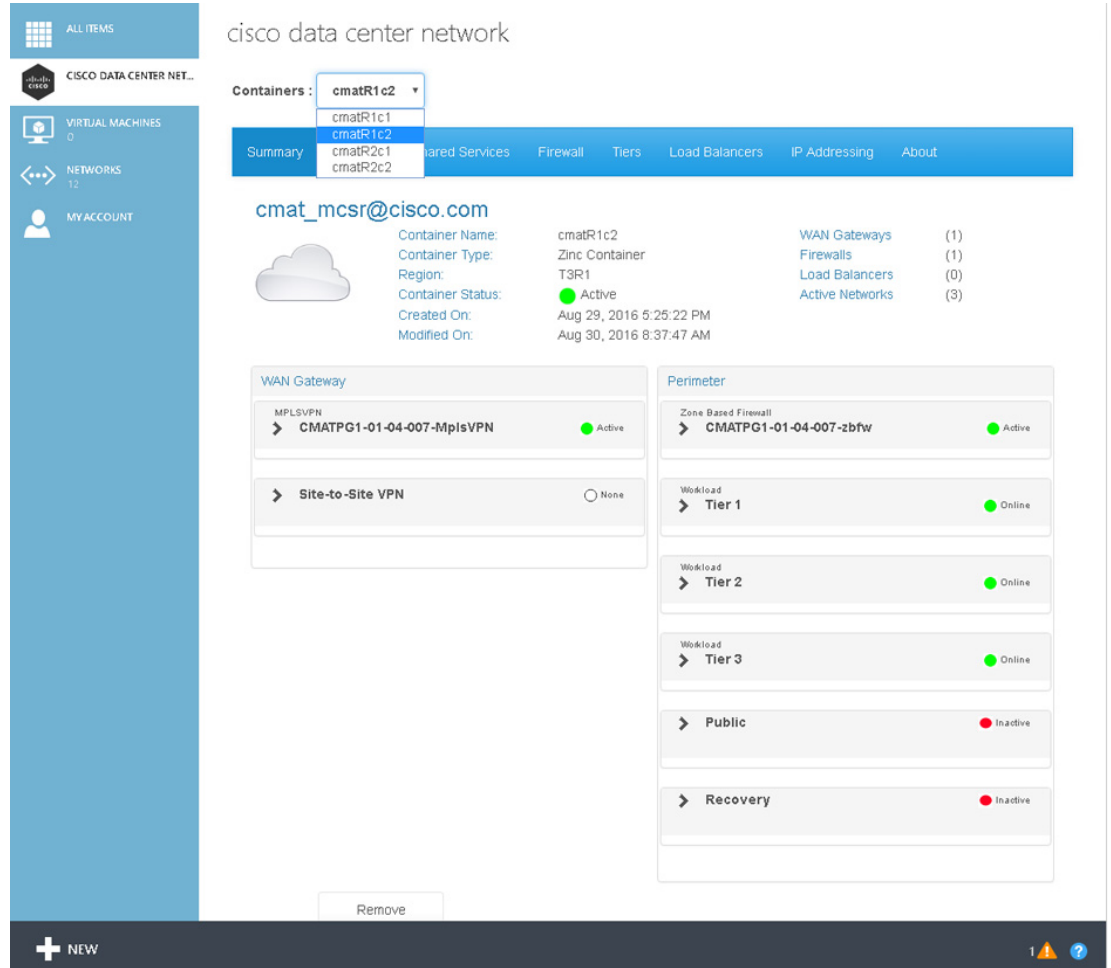
Note

When you delete a container, all information about the container is deleted from the Cisco CNAP database and none of the deleted information can be recovered.

Step 1

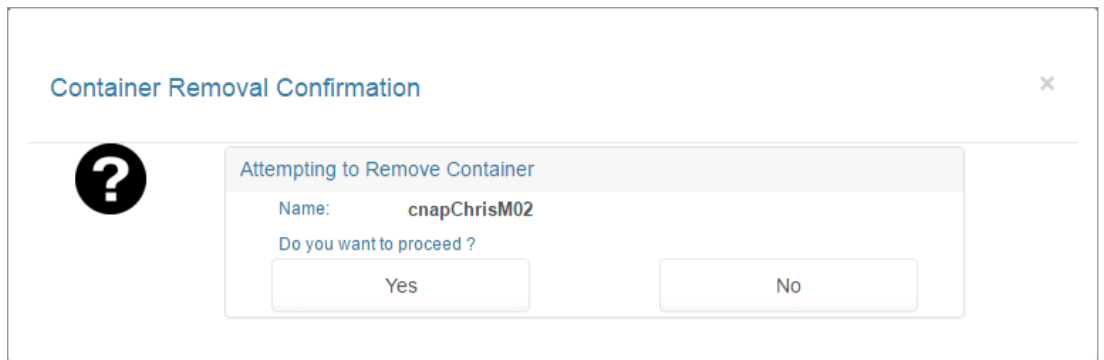
To display summary information about a specific container instance, click **Cisco Network**. You see the Tenant Summary Tab screen.

Figure 2-5 Tenant Summary Tab Screen



Step 2 You can use the Containers: pull-down menu to select a different container to delete. To delete the selected container, at the bottom of the screen click **Remove**.
 You see a screen asking you to confirm the deletion, as shown in the following screen.

Figure 2-6 Confirm Container Deletion



Step 3 Click **Yes** to delete the container or **No** to cancel the deletion.

Viewing Gateway Information about a Container

Step 1 To view gateway information for the currently selected container, click the **Gateway** tab. You see the Tenant Gateway screen. The screen below shows an example for MPLS.

Figure 2-7 Tenant Gateway Tab Screen—MPLS

The screenshot displays the 'Tenant Gateway Tab Screen' for an MPLS gateway. The interface includes a left-hand navigation menu with categories like 'ALL ITEMS', 'CISCO DATA CENTER NET.', 'VIRTUAL MACHINES', 'NETWORKS', and 'MYACCOUNT'. The main area shows the 'cisco data center network' with a 'Containers' dropdown set to 'cmatR1c2'. A horizontal tab bar contains 'Summary', 'Gateway', 'Shared Services', 'Firewall', 'Tiers', 'Load Balancers', 'IP Addressing', and 'About', with 'Gateway' currently selected. Under the 'Gateways' section, 'MPLS' is expanded to show 'Internet' and 'Site-to-Site'. The 'CMATt3r1MCSR WAN Gateway' is highlighted, showing its status as 'Active' and various configuration parameters for the 'MPLS VPN Backbone' and 'PE' sections. A 'Remove' button is located at the bottom of the gateway details.

You can perform the following operation on the gateway screen:

- Remove Button—To remove a gateway, click **Remove**.

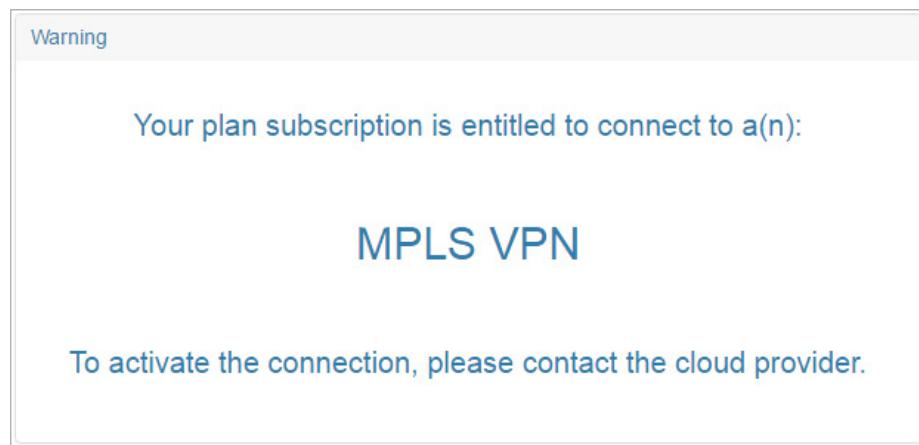
The screen displays the following information:

- Tenant:—Displays the tenant name.
- Container Type:—Displays the container type name, which in the current release is limited to Zinc.
- Region:—Displays the Region name.

- Status:—Displays the WAN Gateway status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
 - Green—WAN Gateway is Active.
 - Red—WAN Gateway is Inactive.
 - Yellow—WAN Gateway state is Creating.
- Name:—Displays the name in the form <abbreviation>-mpls-vpn.
- Gateway Type:—MPLS VPN
- Description:—Descriptive name.
- MPLS VPN Backbone:
 - Aut. System Number—The PEaciL2InterfacePrimary field from the global settings (contact your cloud provider for more information about this field).
 - Network ID—VLAN ID.
 - Import Route Target—Configured RT for the WAN Gateway.
 - Export Route Target—Configured RT for the WAN Gateway.
 - Route Descriptor—Configured descriptor based on your cloud provider's network design.
- PE:
 - VRF—Generated by Cisco CNAP based on the abbreviation of the container ID.
 - Primary IP—External PE IP Address in dotted format.
 - Secondary IP—External PE IP Address in dotted format.
 - Mask—External PE Mask in dotted format

Step 2 If the WAN Gateway has not been activated, you see the following screen.

Figure 2-8 Gateway Tab—MPLS WAN Gateway Not Activated



Step 3 Contact your cloud provider to have the WAN Gateway activated.

Setting up an Internet WAN Gateway

If your cloud provider has enabled Internet WAN Gateway for the plan, you can:

- Enable an Internet WAN Gateway.
- Enable Internet access for all or specific tiers.
- Disable Internet access for all tiers.
- Disable the Internet WAN Gateway.

To set up and manage an Internet WAN gateway:

Step 1 Click the **Gateway** tab, then under Gateways, click **Internet**. You see the following screen.

Figure 2-9 Internet WAN Gateway

The screenshot displays the configuration page for an Internet WAN Gateway in the Cisco Cloud Network Automation Provisioner. The page title is "cisco data center network" and the container is "cmat03scsr". The navigation tabs include Summary, Gateway, Shared Services, Firewall, Tiers, Load Balancers, IP Addressing, and About. The "Gateway" tab is active, and the "Internet" gateway type is selected under "Gateways".

The configuration details for the "Internet WAN Gateway" are as follows:

- Enabled:** Enabled
- Tenant Loopback Interface:**
 - Name: [Text Input]
 - Primary IP: [Text Input]
 - Secondary IP: [Text Input]
 - Mask: [Text Input]
- Access:**
 - Allow workloads to Access Internet
 - Dynamic NAT Subnet: [Text Input]
- Workload Tier Segments:**

Tier	Network	Name	Description

Buttons for "Save" and "Edit" are visible at the bottom of the configuration area.

Step 2 Click the check box next to **Enabled**, as shown in the following screen.

Figure 2-10 Internet WAN Gateway Tab—Enabled Box Checked

The screenshot shows the configuration page for an Internet WAN Gateway in the Cisco Cloud Network Automation Provisioner. The interface includes a left-hand navigation menu with options like 'ALL ITEMS', 'VIRTUAL MACHINES', 'NETWORKS', and 'MY ACCOUNT'. The main content area is titled 'Internet WAN Gateway' and shows the following configuration:

- Enabled:** Enabled
- Tenant Loopback Interface:**
 - Name: Loopback0
 - Primary IP: 12.1.1.79
 - Secondary IP: 12.1.1.80
 - Mask: 255.255.255.255
- Access:**
 - Allow workloads to Access Internet
 - Dynamic NAT Subnet: [Empty field]
 - Workload Tier Segments table:

Tier	Network	Name	Description

At the bottom of the configuration area is a 'Save' button. The bottom status bar shows a '+ NEW' button, a notification icon with '1', and a help icon.

The interface information is automatically populated, but it is not applied until you click **Save**.

Step 3 Click the check box next to **Allow workloads to Access Internet**, as shown in the following screen.

215720

Figure 2-11 Internet WAN Gateway Tab—Allow Workload Access Box Checked

The screenshot shows the configuration page for an Internet WAN Gateway. The 'Access' section has the checkbox 'Allow workloads to Access Internet' checked. Below it, the 'Dynamic NAT Subnet' field is empty. The 'Workload Tier Segments' section contains an empty table with columns for Tier, Network, Name, and Description. An 'Edit' button is located below the table. A 'Save' button is at the bottom of the configuration area.

Tier	Network	Name	Description
------	---------	------	-------------

Step 4 Click the **Edit** button to select the Tiers that will have access, as shown in the following screen.

Figure 2-12 Internet WAN Gateway Tab—Select Tiers for Access

The 'Available Segments' dialog box shows two tables: 'Deny Access' and 'Permit Access'. The 'Deny Access' table has three rows, with the first row highlighted. The 'Permit Access' table is empty. There are 'Select >>' and '<< Unselect' buttons between the tables. 'Save' and 'Cancel' buttons are at the bottom.

Tier	Network	Name
Tier 1	10.5.1.0/24	Seg 1
Tier 2	10.5.2.0/24	Seg 1
Tier 3	10.5.3.0/24	Seg 1

Step 5 Click a Tier to highlight it, then click the **Select>>** button to move it to the Permit Access column. Repeat for each Tier that you want to have access. When you are finished, click the **Save** button. The Tiers with Internet access are shown on the Internet Gateway tab, as shown in the following screen.

Figure 2-13 Internet WAN Gateway Tab—Tiers with Access Displayed

The screenshot shows the configuration page for the Internet WAN Gateway. The interface includes a left-hand navigation menu with options like 'ALL ITEMS', 'CISCO DATA CENTER NET...', 'VIRTUAL MACHINES', 'NETWORKS', and 'MY ACCOUNT'. The main content area is titled 'Internet WAN Gateway' and shows the following details:

- Tenant:** cmat01scsr@cisco.com
- Container Type:** Zinc Container
- Hosting Cloud:** zinc_cloud
- Status:** Enabled (indicated by a radio button)

The configuration is divided into sections:

- Tenant Loopback Interface:**
 - Name: Loopback0
 - Primary IP: 12.1.1.79
 - Mask: 255.255.255.255
 - Secondary IP: 12.1.1.80
- Access:**
 - Allow workloads to Access Internet
 - Dynamic NAT Subnet: [Empty field]
 - Workload Tier Segments table:

Tier	Network	Name	Description
Tier 1	192.168.1.0/24	Workload Segment 1	Segment 1 Description

Buttons for 'Edit' and 'Save' are located at the bottom of the configuration area.

Step 6 To change the Tiers that have access, click the **Edit** button. You see the following screen.

215723

Figure 2-14 Internet WAN Gateway Tab—Edit Tiers with Access

Available Segments

Deny Access		
Tier	Network	Name
Tier 2	10.5.2.0/24	Seg 1
Tier 3	10.5.3.0/24	Seg 1

Select >>

<< Unselect

Permit Access		
Tier	Network	Name
Tier 1	10.5.1.0/24	Seg 1

Save Cancel

215724

- Step 7** Click a Tier to highlight it, then click the **Select>>** button to move it to the Permit Access column. Repeat for each Tier that you want to have access. To remove Internet access for a Tier, select it in the Permit Access column and click **<<Unselect**. The following screen shows an additional Tier moved to the Permit Access column.

Figure 2-15 Internet WAN Gateway Tab—Add Access for Another Tier

Available Segments

Deny Access		
Tier	Network	Name
Tier 3	10.5.3.0/24	Seg 1

Select >>

<< Unselect

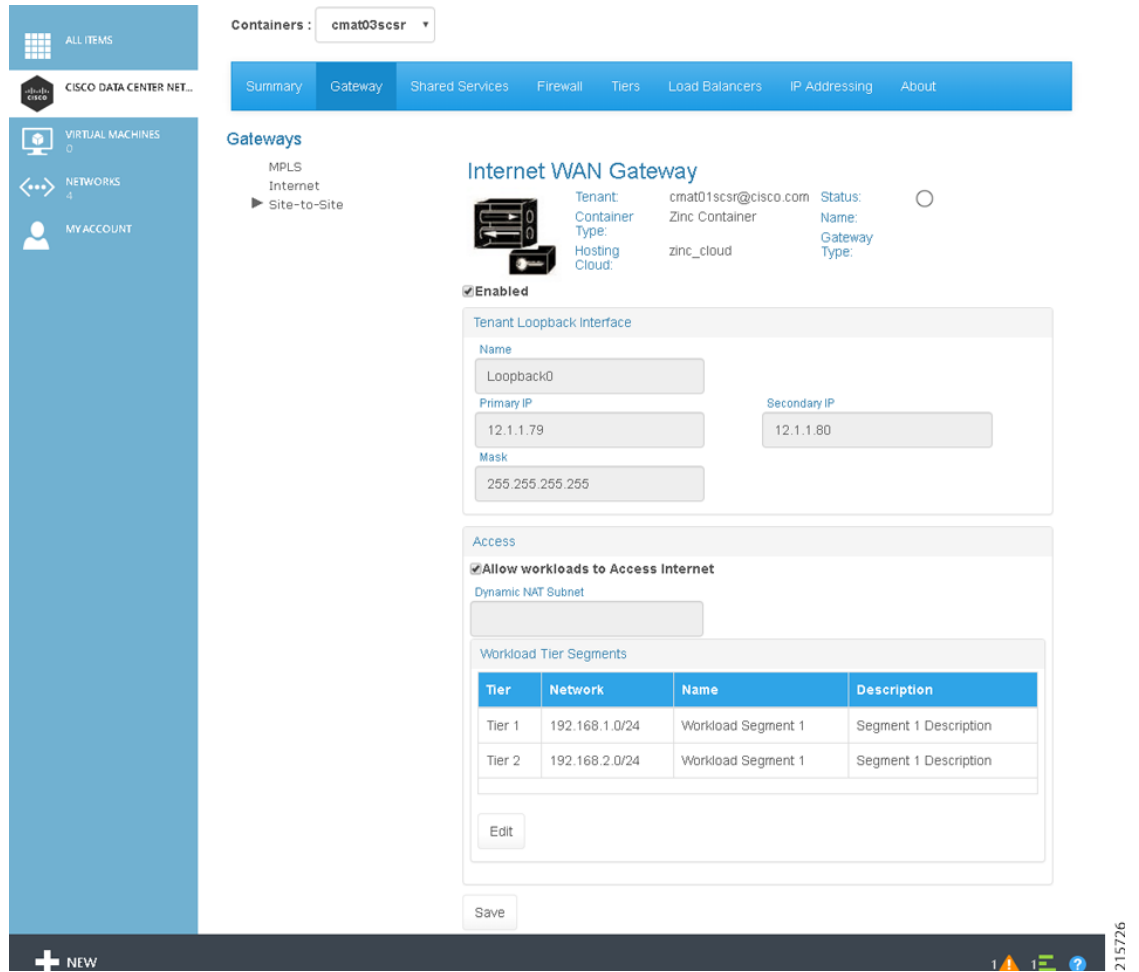
Permit Access		
Tier	Network	Name
Tier 1	10.5.1.0/24	Seg 1
Tier 2	10.5.2.0/24	Seg 1

Save Cancel

215725

- Step 8** When you are finished, click the **Save** button. The Tiers with Internet access are shown on the Internet Gateway tab, as shown in the following screen.

Figure 2-16 Internet WAN Gateway Tab—Additional Tiers with Access Displayed



If you had allowed Internet access for all Tiers, they would all appear on the Internet Gateway tab, as shown in the following screen.

Figure 2-17 Internet WAN Gateway Tab—All Tiers with Access Displayed

The screenshot shows the 'Internet WAN Gateway' configuration page in the Cisco Cloud Network Automation Provisioner. The page is divided into several sections:

- Summary:** Shows the gateway is 'Enabled' and 'Active'. It lists the Tenant as 'cmat01scsr@cisico.com', Container Type as 'Zinc Container', and Hosting Cloud as 'zinc_cloud'. The Gateway Type is 'Internet Access'.
- Tenant Loopback Interface:** Shows the Name as 'Loopback0', Primary IP as '12.1.1.71', Secondary IP as '12.1.1.72', and Mask as '255.255.255.255'.
- Access:** Shows the checkbox 'Allow workloads to Access Internet' is checked. The Dynamic NAT Subnet is '11.1.1.0/24'.
- Workload Tier Segments:** A table with 4 columns: Tier, Network, Name, and Description. It lists four tiers: Tier 1, Tier 2, Tier 3, and DMZ Tier 1, each with a corresponding network and description.

At the bottom of the page, there is a 'Save' button and a '+ NEW' button. The page number '215727' is visible in the bottom right corner.

Step 9 When you are finished modifying Tiers, click **Save** on the main Internet WAN Gateway tab.

Step 10 To disable Internet access for all Tiers, uncheck the check box next to **Allow workloads to Access Internet**, then click **Save**, as shown in the following screen.

Figure 2-18 Internet WAN Gateway Tab—Disable Access to All Tiers

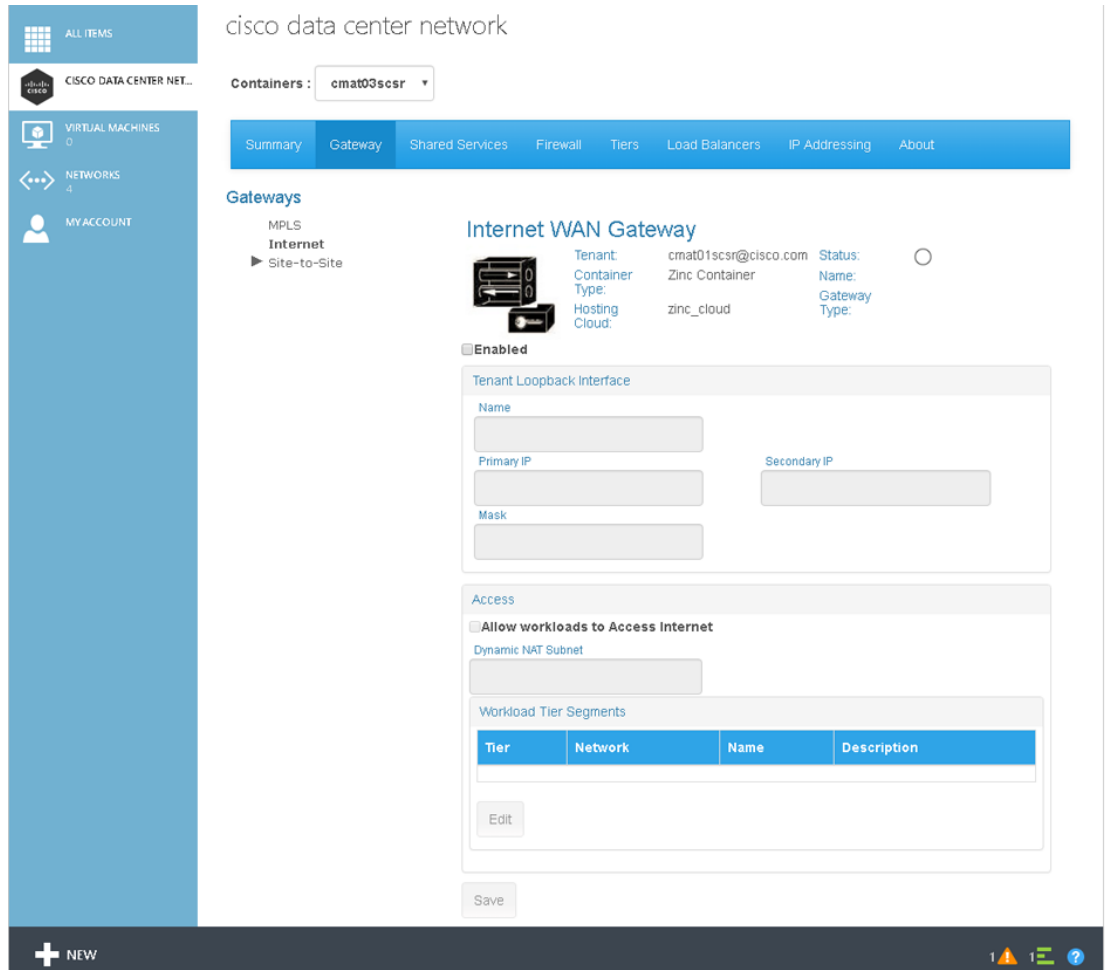
The screenshot displays the configuration page for the 'Internet WAN Gateway' in the Cisco Cloud Network Automation Provisioner. The interface is titled 'cisco data center network' and shows the container 'cmat03scsr'. The 'Gateway' tab is active, and the gateway is currently 'Enabled'. The configuration includes a tenant loopback interface 'Loopback0' with a primary IP of 12.1.1.79 and a mask of 255.255.255.255. The 'Access' section has the checkbox 'Allow workloads to Access Internet' unchecked. Below this is a table for 'Workload Tier Segments' with columns for Tier, Network, Name, and Description. The interface also features a sidebar with navigation options and a bottom status bar with a 'NEW' button and system icons.

Step 11 To disable the Internet WAN Gateway, uncheck the check box next to **Enabled**, as shown in the following screen.



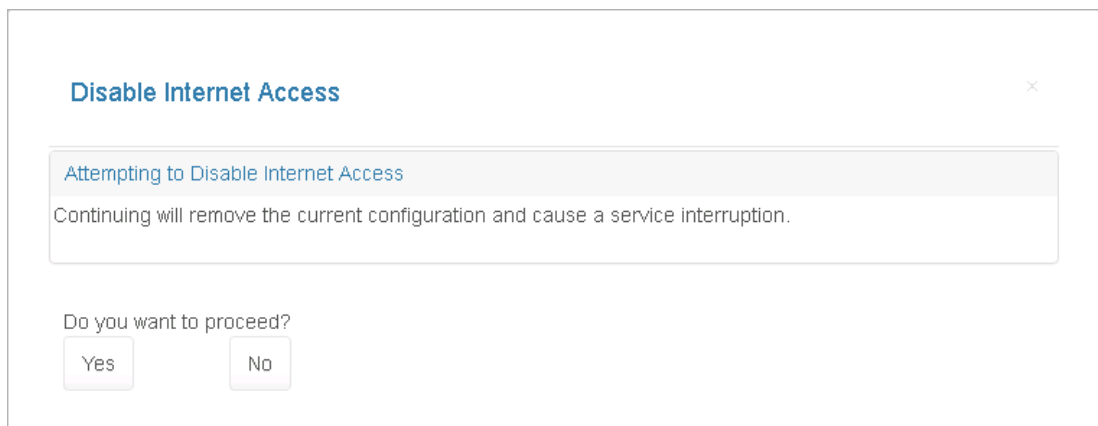
Note If you disable the Internet WAN Gateway, then site-to-site access will not work.

Figure 2-19 Internet WAN Gateway Tab—Disable Internet WAN Gateway



When you click **Save**, you see the following confirmation screen.

Figure 2-20 Internet WAN Gateway Tab—Disable Internet Gateway Confirmation Screen



Step 12 To disable the Internet WAN Gateway, click **Yes**. You see the following screen with the Internet WAN Gateway disabled.

Figure 2-21 Internet WAN Gateway Tab—Internet WAN Gateway Removed

The screenshot displays the configuration page for an Internet WAN Gateway in a cloud provider's tenant portal. The interface is organized into several sections:

- Navigation:** A left sidebar contains menu items like 'ALL ITEMS', 'CISCO DATA CENTER NET...', 'VIRTUAL MACHINES', 'NETWORKS', and 'MY ACCOUNT'. A top navigation bar includes tabs for 'Summary', 'Gateway', 'Shared Services', 'Firewall', 'Tiers', 'Load Balancers', 'IP Addressing', and 'About'.
- Gateway Overview:** A 'Gateways' section shows a tree view with 'MPLS' and 'Internet' (selected), and a sub-item 'Site-to-Site'. The main title is 'Internet WAN Gateway'.
- Configuration Details:**
 - Tenant Information:** Tenant: cmat01scsr@cisico.com, Container: Zinc Container, Type: zinc_cloud, Hosting Cloud: zinc_cloud, Status: (off), Gateway Type: (off).
 - Tenant Loopback Interface:** Fields for Name, Primary IP, Secondary IP, and Mask.
 - Access:** A checkbox for 'Allow workloads to Access Internet' and a 'Dynamic NAT Subnet' field.
 - Workload Tier Segments:** A table with columns: Tier, Network, Name, Description. An 'Edit' button is below it.
- Footer:** A 'Save' button is at the bottom of the configuration area. The bottom of the page shows a '+ NEW' button and system status icons.

Setting up a Site-to-Site VPN

If your cloud provider has enabled Site-to-Site VPN for the plan, you can:

- Enable a Site-to-Site VPN.
- Disable a Site-to-Site VPN.

To set up Site-to-Site VPN:

Step 1 Click the **Gateway** tab, then under Gateways, click **Site-to-Site**. You see the following screen.

Figure 2-22 Site-to-Site VPN Screen

Step 2 Complete the following fields:

- IKE Policy:
 - Encryption—Encryption used for the IKE proposal; used to ensure the secrecy of data during traffic flow: AES, DES, or Triple DES.
 - Hash—Specifies the hash algorithm within an IKE policy; used to authenticate data during traffic flow: MD5, SHA, or SHA256.
 - Keep Alive—Number of seconds during which traffic is not received from the peer before keep-alive messages are sent if there is data traffic to send.
 - Retry—Number of seconds between keep-alive packet retries if the keep-alive message fails.
 - Group—Specify which Diffie-Hellman Modulus Group to use.
- Authentication:
 - Method—Pre-Shared Key: Allow for a secret key to be shared between two peers for mutual authentication prior to tunnel activation.
 - Shared Key—The shared secret for authentication. The shared key must be configured and equal at each peer or the IKE SA cannot be established.
- Transformation Set: ESP Encryption Transform

- esp-des—ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm (no longer recommended).
- esp-3des—ESP with the 168-bit DES encryption algorithm (3DES or Triple DES) (no longer recommended).
- esp-null—Null encryption algorithm.
- esp-aes—SP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm.
- esp-aes-192—SP with the 192-bit Advanced Encryption Standard (AES) encryption algorithm.
- esp-aes-256—SP with the 256-bit Advanced Encryption Standard (AES) encryption algorithm.
- Transformation Set: ESP Authentication Transform
 - esp-md5-hmac—ESP with the MD5 (HMAC variant) authentication algorithm (no longer recommended).
 - esp-sha-hmac—ESP with the SHA (HMAC variant) authentication algorithm.
- Transformation Set: Ah Transform
 - ah-md5-hmac—AH with the MD5 (Message Digest 5) (an HMAC variant) authentication algorithm (no longer recommended).
 - ah-sha-hmac—AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.

Step 3 When you are finished, click **Add Tunnel**.

Removing a MPLS WAN Gateway

To remove a MPLS WAN Gateway, on the MPLS WAN Gateway tab, click **Remove**.

Viewing and Modifying Firewall Information about a Container

On the Firewall tab, you can:

- View summary information about a firewall
- View the hierarchy of information on the Firewall tab
- Configure a firewall
- Change the policy map for a service policy
- Add a new class map
- Change a class map
- Create a new network ACL
- Change an ACL
- Create a new object group
- Change an object group

Understanding Firewall Creation

A firewall is created by default the moment your cloud provider creates a WAN Gateway. Cisco CNAP will automatically set up a perimeter around each of the zones in your container. Each Tier is considered a zone, as is the Layer 3 VPN as well as any other external access such as Site-to-Site VPN, Internet access, etc. The Firewall tab will not display any information until the WAN Gateway has been provisioned, since there is no point in showing how traffic is going to be regulated if you cannot access the container from the “outside”.

For detailed information on the base firewall configuration, see: *Cisco Cloud Architecture for the Microsoft Cloud Platform: Zinc Container Configuration Guide, Release 1.0*

http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/IaaS_Zinc_Config/CCAMCP1_IaaS_Zinc_Config.html

Viewing Summary Information about a Firewall

-
- Step 1** To view firewall information, click the **Firewall** tab.
You see the following screen.

Figure 2-23 Firewall Tab

The screenshot shows the 'Firewall' tab for a container named 'cmatR1c2'. The interface includes a navigation sidebar on the left with options like 'ALL ITEMS', 'CISCO DATA CENTER NET...', 'VIRTUAL MACHINES', 'NETWORKS', and 'MY ACCOUNT'. The main content area displays the following information:

Tenant	Region	Status
cmat_mcsr@cisco.com	T3R1	Active
Container Type	Name	Created/Modified On
Zinc Container	CMATPG1-01-04-007-zbfw	Aug 30, 2016 8:36:19 AM Aug 30, 2016 8:36:19 AM

Below the metadata table, there is a 'Zone Pair' section with two dropdown menus for 'Source Zone' and 'Destination Zone'.

The screen displays the following information:

- Tenant:—Displays the tenant name.
- Container Type:—Displays the container type instance name.
- Region:—Displays the Region name.
- Modified:—Displays the date and time when the firewall was last modified.
- Status:—Displays the firewall status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
 - Green—Firewall is Active.
 - Red—Firewall is Inactive.
 - Yellow—Firewall state is Creating.
- Name:—Displays the name in the form <abbreviation>-fw.
- Created:—Displays the date and time when the firewall was created.
- Zone Pair—Source Zone and Destination Zone are the zones between which the firewall is configured.

299966

Viewing the Hierarchy of Information on the Firewall Tab

You use the Firewall Tab to view the various layers of information about firewalls, including:

- Service Policy with its associated Policy Map for a particular Source Zone and Destination Zone



Note To change the Policy Map associated with a Source and Destination Zone pair, you have to define a new Policy Map, which replaces the existing one.

- Class Maps in a Service Policy
- Access Control Lists within a Class Map
- Rules in an Access Control List
- Object Groups of a Rule

To display the various tiers of information about a firewall:

-
- Step 1** Use the Source Zone: and Destination Zone: pull-down menus to select the relevant zones, as shown in the following screens.

Figure 2-24 Firewall Source Zone Pull-down Menu

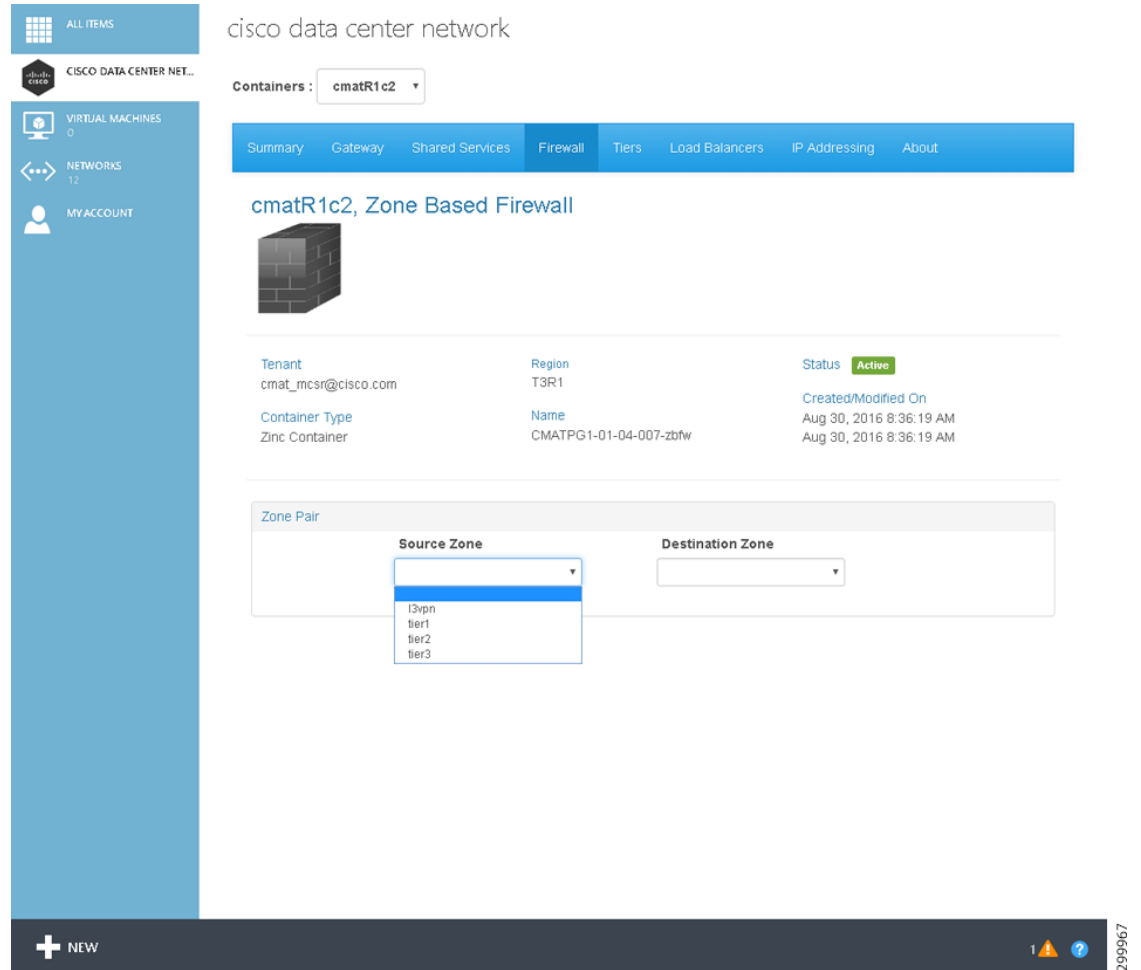


Figure 2-25 Firewall Destination Zone Pull-down Menu

The screenshot displays the Cisco Cloud Network Automation Provisioner interface. The left sidebar contains navigation options: ALL ITEMS, CISCO DATA CENTER NET..., VIRTUAL MACHINES (0), NETWORKS (12), and MYACCOUNT. The main content area shows the 'cisco data center network' with a 'Containers' dropdown set to 'cmatR1c2'. A blue navigation bar includes tabs for Summary, Gateway, Shared Services, Firewall (selected), Tiers, Load Balancers, IP Addressing, and About. Below this, the page title is 'cmatR1c2, Zone Based Firewall' with a brick icon. A metadata table provides details:

Tenant	Region	Status
cmat_mcsr@cisco.com	T3R1	Active
Container Type	Name	Created/Modified On
Zinc Container	CMATPG1-01-04-007-zbfw	Aug 30, 2016 8:36:19 AM Aug 30, 2016 8:36:19 AM

The 'Zone Pair' section features two dropdown menus: 'Source Zone' (set to 'I3vpn') and 'Destination Zone' (with a pull-down menu open showing 'tier1', 'tier2', and 'tier3'). The bottom of the interface includes a '+ NEW' button, a notification icon with '1', a help icon, and the ID '2099968'.

After you select the Source and Destination Zones, the screen populates with a variety of information, as shown in the following screen.

Figure 2-26 Firewall Zones Selected Screen—Detailed Firewall Information Displayed

The various operations you can perform on this screen are described in the following section, [Configuring a Firewall](#).

Step 2 If you click an element on the screen to bring it into focus, it changes to blue. For the element in focus:

- The **Remove** button de-couples the entity in focus, for example the Class Map Instance tier1-web, from the parent entity marked, for example the Policy Map l3vpn-to-tier1 for the Service Policy.

The **Remove** button may be used to remove a:

- Class Map Instance from a Policy Map
- Access List from a Class Map
- Rule from an Access List



Note In the current release, Cisco CNAP allows and requires you to associate only one Policy Map with any given zone pair. Consequently, the **Remove** button is deactivated when you drill down to the Policy Map, but not further.

- The **Modify** button displays the change screen for the element currently in focus.

Configuring a Firewall



Note

You can only configure a firewall after you have created a container and your cloud provider has created a WAN Gateway. The firewall is automatically created with a base configuration either during container creation if the container has multiple tiers or when the WAN gateway is created. For more information, see the section Understanding Firewall Creation.

Firewalls are configurable on a per-Tier basis. You configure one firewall per container (not per tier) and you specify policy rules between zones. Firewall policies are specified between each of the workload Tiers and outside interfaces and in each direction independently. That is, a policy needs to be specified for L3VPN to Tier 1 and Tier 1 to L3VPN, and so on for each tier.

To configure a firewall for a container:

- Step 1** Use the Source Zone: and Destination Zone: pull-down menus to select the relevant zones. After you select the zones, the screen populates with a variety of information, as shown in the following screen.

Figure 2-27 Firewall Zones Selected Screen—Detailed Firewall Information Displayed

The screenshot displays the 'Zone Pair' configuration screen in the Cisco Cloud Network Automation Provisioner. The interface includes a left-hand navigation menu with categories like 'ALL ITEMS', 'CISCO DATACENTER NETW...', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'PLANS', and 'USER ACCOUNTS'. The main content area shows the following configuration details:

Zone Pair

Source Zone: l3vpn
Destination Zone: tier1
Reset

Service Policy

Name: l3vpn-to-tier1

Class Map Instance

Name	Action	Log Drop	Filter
- tier1-web	inspect	<input checked="" type="checkbox"/>	match-any
+ default-service	inspect	<input checked="" type="checkbox"/>	match-any
class-default	drop	<input checked="" type="checkbox"/>	match-all

Access Group

Name	Action	Target	Source	Destination
- tier1-web-acl	permit	web (obj)	any	tier1-subnet (obj)

Object Groups

Name	Target	Filter	Port	Range
- web	tcp	eq	www	
+ tier1-subnet	tcp	eq	443	

Buttons: ADD, MODIFY, REMOVE

Bottom bar: + NEW

215545

Step 2 To add a Policy Map, click the Policy Map under Service Policy, then click the **Add** button. You see the following screen.

Figure 2-28 Add Policy Map for Service Policy Screen

The screenshot shows a web interface for configuring a Service Policy. The main heading is "Service Policy" in blue text. Below it, there is a section titled "Policy Map" in a light blue box. Inside this section, there is a text input field labeled "Name". At the bottom right of the form, there are two buttons: "Save" and "Close". A small "X" icon in a square is located in the top right corner of the main form area. On the far right edge of the screenshot, the number "299815" is printed vertically.

Step 3 Enter a name.

As you begin entering a name, the screen expands to display the following screen where you can associate class maps with the new Policy Map.

Figure 2-29 New Policy Map—Class Maps Screen

Service Policy [X]

Policy Map
new-service-policy

Class Map Instance

On Device		Class Map Instances			
Name		Name	Action	Log Drop	Filter
permit-all	Select >	class-default	drop	<input checked="" type="checkbox"/>	match-all
control-protocols	+ New				
dmz-web	<< Unselect				
default-service					
tier1-web					

Save Close

299816

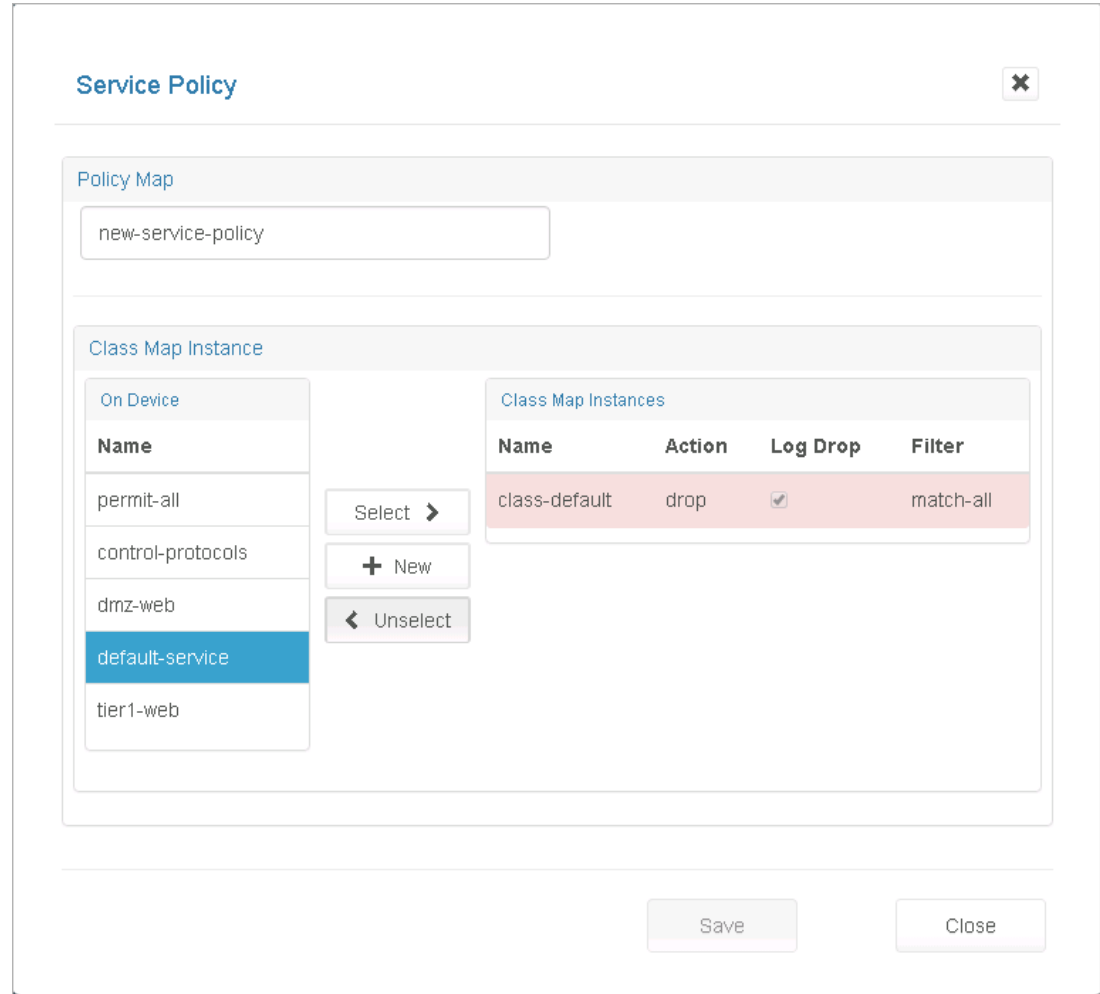
Step 4 Associate class maps with the new Policy Map:

- Name—Enter a descriptive name for the Policy Map.
- On Device—Lists all the Class Maps available on the device.
- Class Map Instances—Lists the class maps associated with this Policy Map.
- **Select**>> button—Click to select one or more Class Maps available “On Device”. Clicking **Select** associates them to the current Policy Map.
- <<**Unselect** button—Click to select one or more Class Map Instances associated with the current Service Policy. Clicking **Unselect** disassociates them from the current Policy Map.
- **+New** button—Click the **+New** button to create a new Class Map.
- Ordering the Class Maps—The Class Map Instances get added to the top of the list. You can reorder them by clicking <<**Unselect** and **Select**>> on the Class Maps in the desired order.

**Note**

The class-default shown in the following screen cannot be de-coupled from the policy.

Figure 2-30 Class Map Instance class-default Screen



Step 5 When you are finished, click **Save**.

Changing a Policy Map for a Service Policy

- Step 1** Click a Policy Map to select it (mark it blue).
- Step 2** Click the **Modify** button to display the Policy Map pop-up.

Figure 2-31 Policy Map Pop-up Screen

Service Policy [Close]

Policy Map

I3vpn-to-tier1

Class Map Instance

On Device

Name
permit-all
control-protocols
dmz-web

Select > + New < Unselect

Class Map Instances

Name	Action	Log Drop	Filter
tier1-web	inspect	<input checked="" type="checkbox"/>	match-any
default-service	inspect	<input checked="" type="checkbox"/>	match-any
class-default	drop	<input checked="" type="checkbox"/>	match-all

Save Close

299819

This is the same as the Create Service Policy page, but with the name field deactivated. You can click:

- **Select>>** to select Class Maps available on the device.
- **<<Unselect** to unselect Class Map Instances associated with the Policy Map.
- **+New** to create a new Class Map.

Adding a New Class Map

Step 1 Click **+New** in the Class Map Instance section on the Policy Map screen shown below.

Figure 2-32 Class Map Instance Screen—Click +New

The screenshot shows the 'Service Policy' configuration interface. At the top, there is a 'Policy Map' section with a text input field containing 'l3vpn-to-tier1'. Below this is the 'Class Map Instance' section, which is divided into two parts:

- On Device:** A list of class maps: 'permit-all', 'control-protocols', and 'dmz-web'. To the right of this list are three buttons: 'Select >', '+ New', and '< Unselect'.
- Class Map Instances:** A table with the following data:

Name	Action	Log Drop	Filter
tier1-web	inspect	<input checked="" type="checkbox"/>	match-any
default-service	inspect	<input checked="" type="checkbox"/>	match-any
class-default	drop	<input checked="" type="checkbox"/>	match-all

At the bottom of the screen, there are two buttons: 'Save' and 'Close'.

You see the following screen.

Figure 2-33 New Class Map Instance Screen

The screenshot shows the 'Class Map Instance' configuration interface. At the top, there is a 'Class Map' section with a text input field labeled 'Name'. At the bottom of the screen, there are two buttons: 'Update' and 'Cancel'.

Step 2 In the Name field, enter a descriptive name for your new Class Map.

This expands the screen to display the following screen.

Figure 2-34 New Class Map Instance Details Screen

The fields on this screen are:

- **match-all/match-any**—This pull-down menu identifies the criteria used to match access groups in the map.
- **On Device**—Lists all the ACLs available for use on the device.
- **ACL Instances**—Lists the ACLs associated with this Class Map.
- **Select>>**, **+New**, and **<<Unselect**—These buttons work the same as on the Service Policy screen.

Step 3 When you are finished associating ACLs to this Class Map, click **Update** to return to the Service Policy screen.

Changing a Class Map

Step 1 Select the desired Class Map on the Firewall tab.

Step 2 Click **Modify**.

You see the following screen.

Figure 2-35 Class Map Instance Screen

The screenshot shows the 'Class Map Instance' configuration screen. At the top, there is a title bar with the text 'Class Map Instance' and a close button (X). Below the title bar, there are two input fields: the first contains 'tier1-web' and the second is a dropdown menu showing 'match-any'. Below these fields is a section titled 'Access Group'. This section contains two tables. The left table is titled 'On Device' and has a 'Name' column with three entries: 'default-service-acl', 'dmz-web-acl', and 'permit-all-acl'. The right table is titled 'ACL Instances' and has columns for 'Name', 'Target', and 'Action', with one entry: 'tier1-web-acl'. Between the two tables are three buttons: 'Select >', '+ New', and '< Unselect'. At the bottom right of the screen are two buttons: 'Save' and 'Close'.

This screen is identical to the Create Class Map pop up, but with the Name field deactivated.

Step 3 You can:

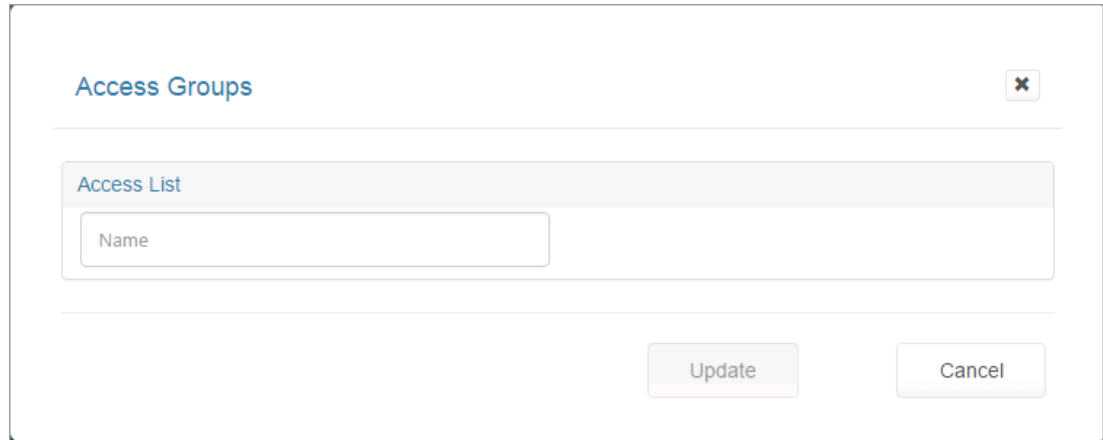
- **Select**>> ACLs from the list of ACLs available on the device.
- <<**Unselect** ACLs associated with the Class Map.
- Create a **+New** ACL on the device and have it associated with the Class Map.

9824

Creating a New Network Access Control List

- Step 1** Click **New** on the Class Map Instance screen shown above, which displays the Access Group screen shown below.

Figure 2-36 Access Groups Screen



The screenshot shows a web interface titled "Access Groups" with a close button (X) in the top right corner. Below the title is a section labeled "Access List" containing a text input field with the placeholder text "Name". At the bottom of the form are two buttons: "Update" and "Cancel". A vertical text label "299825" is located on the right side of the screenshot.

- Step 2** When you enter a name for the Access List, the screen expands to display the Rules section. Since this is a new ACL, the screen expands in the Add Rule mode as shown below.

Figure 2-37 Access Groups Details Screen

The screenshot displays the 'Access Groups' configuration interface. At the top, the title 'Access Groups' is shown with a close button (x). Below this is the 'Access List' section, which contains a text input field with the value 'new-acl'. The main area is the 'Rules' section, which is currently expanded. It contains several configuration fields:

- Action:** A dropdown menu set to 'permit'.
- Target:** A dropdown menu set to 'ahp'.
- Source:** A dropdown menu set to 'any'.
- Destination:** A dropdown menu set to 'any'.
- Filter:** An empty dropdown menu.
- Port:** An empty text input field.

At the bottom right of the Rules section is a '+ Add Rule' button. At the bottom of the entire screen are 'Update' and 'Cancel' buttons. A small 'x' icon is located in the top right corner of the window.

Step 3 The fields you can complete include:

- Action—Indicates whether traffic is permitted or denied by the rule.
- Target—A valid protocol or object group.
- Source—Network entity identified as the traffic source.
- Destination—Network entity identified as the traffic destination.

Step 4 If you select **Object-Group** in the drop-down menu for Target, the Source or Destination menus allow you to choose from object groups existing on the device or create new ones, as shown in the following screen.

299626

Figure 2-38 Access Groups Screen—Object Group Selected

The screenshot shows the 'Access Groups' configuration interface. At the top, the title 'Access Groups' is displayed with a close button. Below it, the 'Access List' section contains a text input field with the value 'new-acl'. The 'Rules' section is expanded, showing a rule configuration form. The 'Action' dropdown is set to 'permit'. The 'Target' dropdown is set to 'object-group', and the 'Object Group' dropdown is also set to 'object-group'. The 'Source' dropdown is set to 'any', and the 'Destination' dropdown is set to 'any'. The 'Filter' dropdown is empty, and the 'Port' input field is empty. A '+ Add Rule' button is located at the bottom right of the 'Rules' section. At the bottom of the main screen, there are 'Update' and 'Cancel' buttons.

Step 5 Click the **+Add Rule** button to add the current rule being built to the ACL.

Figure 2-39 Rule Added to ACL Screen

The screenshot shows a web interface for configuring Access Groups. At the top, there's a title 'Access Groups' with a close button (X). Below it, there's a section for 'Access List' with a text input field containing 'new-acl'. Underneath is a 'Rules' section with a '+ New Rule' button. A table lists the rules with columns: Remove, Action, Filter, Port, Range, Target, Source, Destination. One rule is present: Action 'permit', Source 'any', Destination 'any'. At the bottom right, there are 'Update' and 'Cancel' buttons.

Remove	Action	Filter	Port	Range	Target	Source	Destination
X	permit					any	any

Step 6 Click **+New Rule** to add more rules.

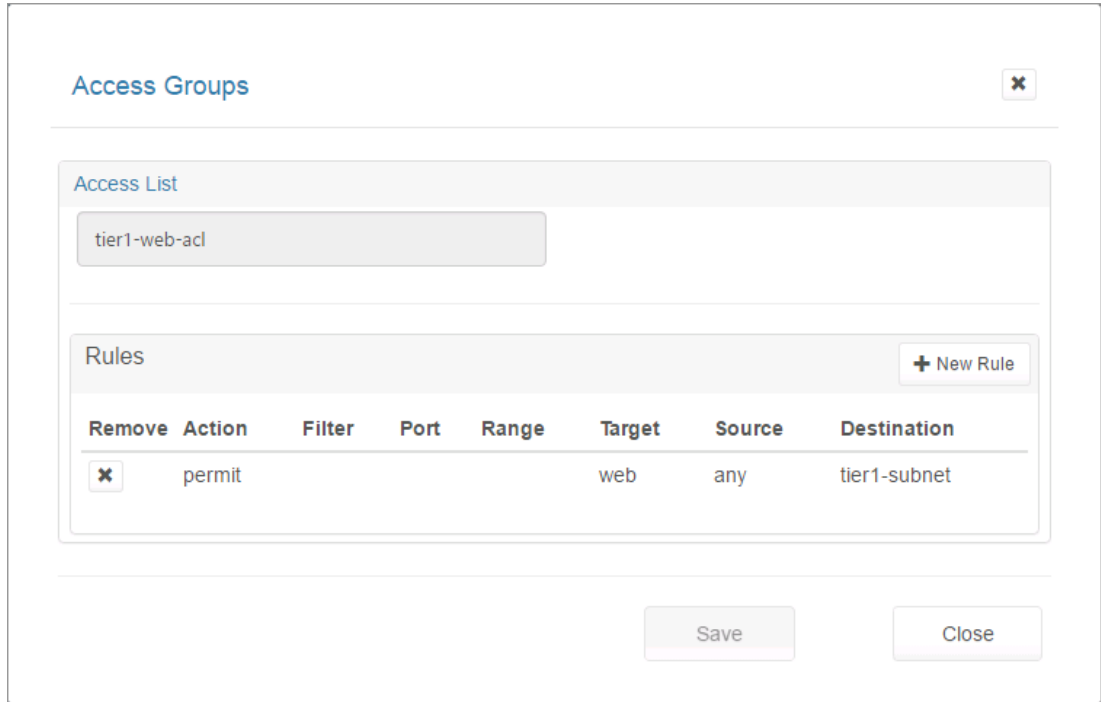
Step 7 Click the **Update** button to exit the Add Rule mode and show the list of all rules in the ACL.

Changing an Access List

Step 1 Select the desired Access List on the Firewall tab.

Step 2 Click **Modify** to display the Access List pop-up screen, as shown below.

Figure 2-40 Access List Pop-up Screen

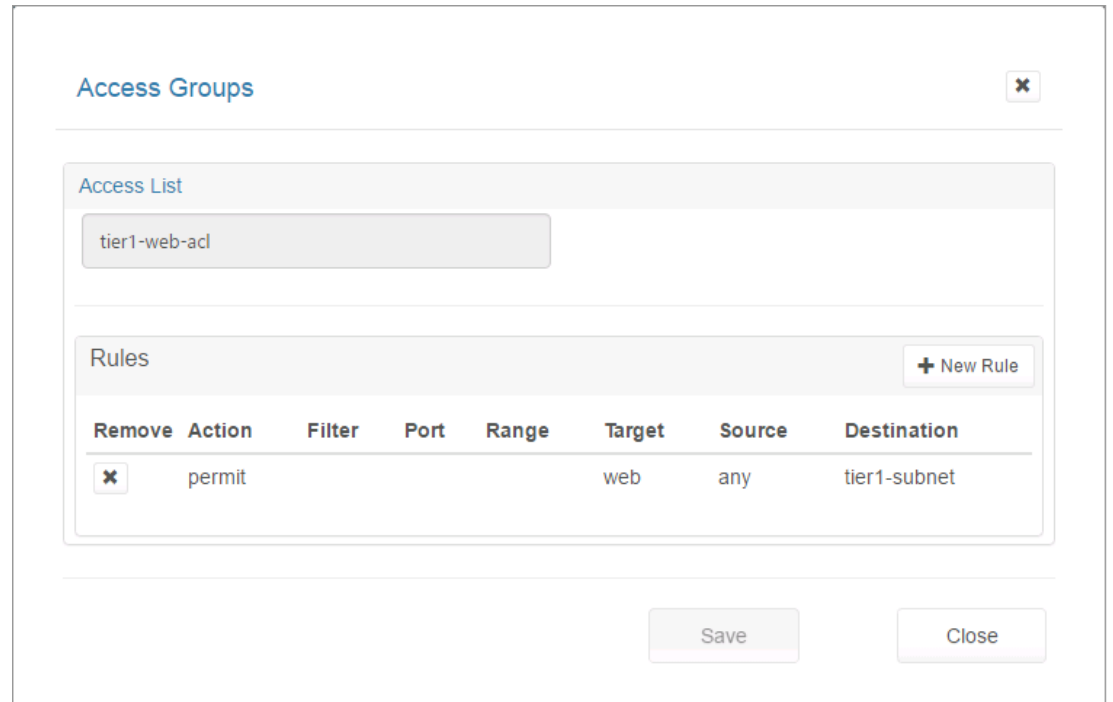


- Step 3** You can add and remove rules as explained in [Creating a New Network Access Control List](#).
- Step 4** If you make any changes to the list of Rules, the **Save** button is activated and you can click it to save the changes.

Creating a New Object Group

- Step 1** Select the desired Access List on the Firewall tab.
- Step 2** Click **Modify** to display the Access List pop-up screen, as shown in the following screen.

Figure 2-41 Access List Pop-up Screen



Step 3 Click the **+New Rule** button.

On the Access Groups screen, the **Target**, **Source**, and **Destination** drop-down menus have an **object-group** option which when selected displays the **Object Group:** fields with drop-down menus with a list of *compatible* object groups and + buttons that launch a page where you can create a new compatible Object Group.

- The Object Group drop-down menu for **Target** would only show Service type Object Groups (groups of objects having the Target, filter, and port fields or having the Target and Range fields).
- The Object Group drop down for **Source** and **Destination** would only show Network type Object Groups (groups of objects having a Host field or having the Subnet and mask fields).
- The + buttons are contextual. Clicking the + button for the **Target** of the ACL Rule launches a page to create an Object Group with Service type objects.
- Clicking the + button for the Source or Destination of the ACL Rule launches a page to create an Object Group with Network type objects.

Step 4 Click the + button as shown in the following screen.

Figure 2-42 Access Groups Screen—Object Group Selected

The screenshot displays the 'Access Groups' configuration interface. At the top, the title 'Access Groups' is shown with a close button (X). Below this, the 'Access List' section contains a single entry: 'tier1-web-acl'. The main 'Rules' section is expanded, showing a rule configuration form. The 'Action' is set to 'permit'. The 'Target' is 'object-group', and the 'Object Group' is also 'object-group'. The 'Source' is 'any', and the 'Destination' is 'any'. The 'Filter' and 'Port' fields are currently empty. A '+ Add Rule' button is located at the bottom right of the rule configuration area. At the very bottom of the screen, there are 'Save' and 'Close' buttons. A vertical reference number '209831' is visible on the right side of the screenshot.

You see the following screen.

Figure 2-43 Object Group Screen

The screenshot shows a web interface for configuring an object group. The main heading is "Object Group" with a close button (X) in the top right corner. Below this heading is a section titled "Object Group" which contains a single text input field with the placeholder text "Name". At the bottom right of the interface are two buttons: "Update" and "Cancel".

Step 5 When you enter a name, you see the Add Object screen, as shown below.

Figure 2-44 Add Object Screen

The screenshot shows the "Add Object" screen within the "Object Group" configuration. The main heading is "Object Group" with a close button (X). Below this heading is a section titled "Object Group" containing a text input field with the value "new-object-group". Below this is a section titled "Objects" which contains a table with three columns: "Target", "Port", and "Range". The "Target" column has a dropdown menu with "Target" selected. The "Port" column has a dropdown menu with "Port" selected. The "Range" column has a text input field with "Range" and a plus sign (+) button. At the bottom right of the interface are two buttons: "Update" and "Cancel".

Step 6 When you click a field, you see information about allowable values, as shown in the following screen.

Figure 2-45 Add Object Screen—Possible Field Values Displayed

The screenshot shows a web interface for adding an object group. The main title is "Object Group" with a close button. Below it, there's a section titled "Object Group" containing a text input field with the value "new-object-group". Underneath is a section titled "Objects" which contains three columns: "Target", "Port", and "Range". The "Target" column has a text input field with "Target" and a dropdown arrow. The "Port" column has a text input field with "Port". The "Range" column has a text input field with "Range" and a "+" button. Below these fields is a note: "Target values are tcp, udp, tcp-udp, icmp or a valid protocol number. If tcp, udp or tcp-udp are chosen then you will need to enter a port or range value. ex icmp". At the bottom right of the form are "Update" and "Cancel" buttons.

Step 7 You can enter information for the following fields:

- Target—A valid protocol {ahp, esp, gre, icmp, ip, tcp, udp, number [0,255]}.
- Filter—eq (equals), gt (greater than), or lt (less than). The Filter indicates the criteria to match packets based on the port number. If “filter” is present, then “port” **must** be present.
- Port—IP port [0,65535]
- Range—*<port-number1>-<port-number2>*. Must be entered from low to high, e.g., 20-90. Match only packets in the range of the port numbers.



Note If “range” is present, the “filter” and “port” properties are ignored.

Step 8 You can create Network or Service type objects and click + to include the object in the group.

A Group **must** be homogeneous; i.e., it must contain objects of only one type (Network or Service)

Step 9 When you click +, you see the following screen.

Figure 2-46 Object Added to Group Screen

The screenshot shows a web interface for managing object groups. At the top, there's a header 'Object Group' with a close button (X). Below it, a text input field contains 'new-object-group'. The main section is titled 'Objects' and contains a table with the following structure:

Remove	Target	Filter	Port	Range
X	tcp	eq	1000	

Below the table, there are 'Update' and 'Cancel' buttons. A vertical label '2958R-35' is visible on the right side of the screenshot.

Step 10 Click the X under **Remove** to remove an object from the group.

Changing an Object Group

Step 1 On the screen shown below, select the object group you want to change, then click **Modify**.

Figure 2-47 Firewall Zones Selected Screen—Select Object Group

The screenshot shows the Cisco Cloud Network Automation Provisioner interface. On the left is a navigation menu with categories like ALL ITEMS, CISCO DATACENTER NEW, WEB SITE CLOUDS, VM CLOUDS, SERVICE BUS CLOUDS, SQL SERVERS, MYSQL SERVERS, AUTOMATION, PLANS, and USER ACCOUNTS. The main content area is titled 'Zone Pair' and shows the following configuration:

Zone Pair

Source Zone: i3vpn
Destination Zone: tier1
Reset

Service Policy

Name: - i3vpn-to-tier1

Class Map Instance

Name	Action	Log Drop	Filter
- tier1-web	inspect	<input checked="" type="checkbox"/>	match-any
+ default-service	inspect	<input checked="" type="checkbox"/>	match-any
class-default	drop	<input checked="" type="checkbox"/>	match-all

Access Group

Name	Action	Target	Source	Destination
- tier1-web-acl	permit	web (obj)	any	tier1-subnet (obj)

Object Groups

Name	Target	Filter	Port	Range
- web	tcp	eq	www	
+ tier1-subnet	tcp	eq	443	

At the bottom of the configuration area are buttons for ADD, MODIFY, and REMOVE. A '+ NEW' button is located at the bottom left of the interface, and a help icon (?) is at the bottom right.

You see the following screen.

215545

Figure 2-48 Modify Object Group Screen

The screenshot shows the 'Object Group' configuration interface. At the top, the group name 'web' is entered. Below this, the 'Objects' section contains a table with the following data:

Remove	Target	Filter	Port	Range
<input type="checkbox"/>	tcp	eq	www	
<input type="checkbox"/>	tcp	eq	443	

At the bottom of the screen, there are 'Save' and 'Close' buttons.

Step 2 You can enter information for the following fields:

- Target—A valid protocol {ahp, esp, gre, icmp, ip, tcp, udp, number [0,255]}.
- Filter—eq (equals), gt (greater than), or lt (less than). The Filter indicates the criteria to match packets based on the port number. If “filter” is present, then “port” **must** be present.
- Port—IP port [0,65535]
- Range—<port-number1>-<port-number2>. Must be entered from low to high, e.g., 20-90. Match only packets in the range of the port numbers.



Note If “range” is present, the “filter” and “port” properties are ignored.

Step 3 You can create Network or Service type objects and click + to include the object in the group.

A Group **must** be homogeneous; i.e., it must contain objects of only one type (Network or Service)

Step 4 When you click +, the object is added to the group. Click the **X** under **Remove** to remove an object from the group. When you are done, click **Save** to save your changes or **Close** to exit without saving them.

Viewing and Modifying Tier Information about a Container

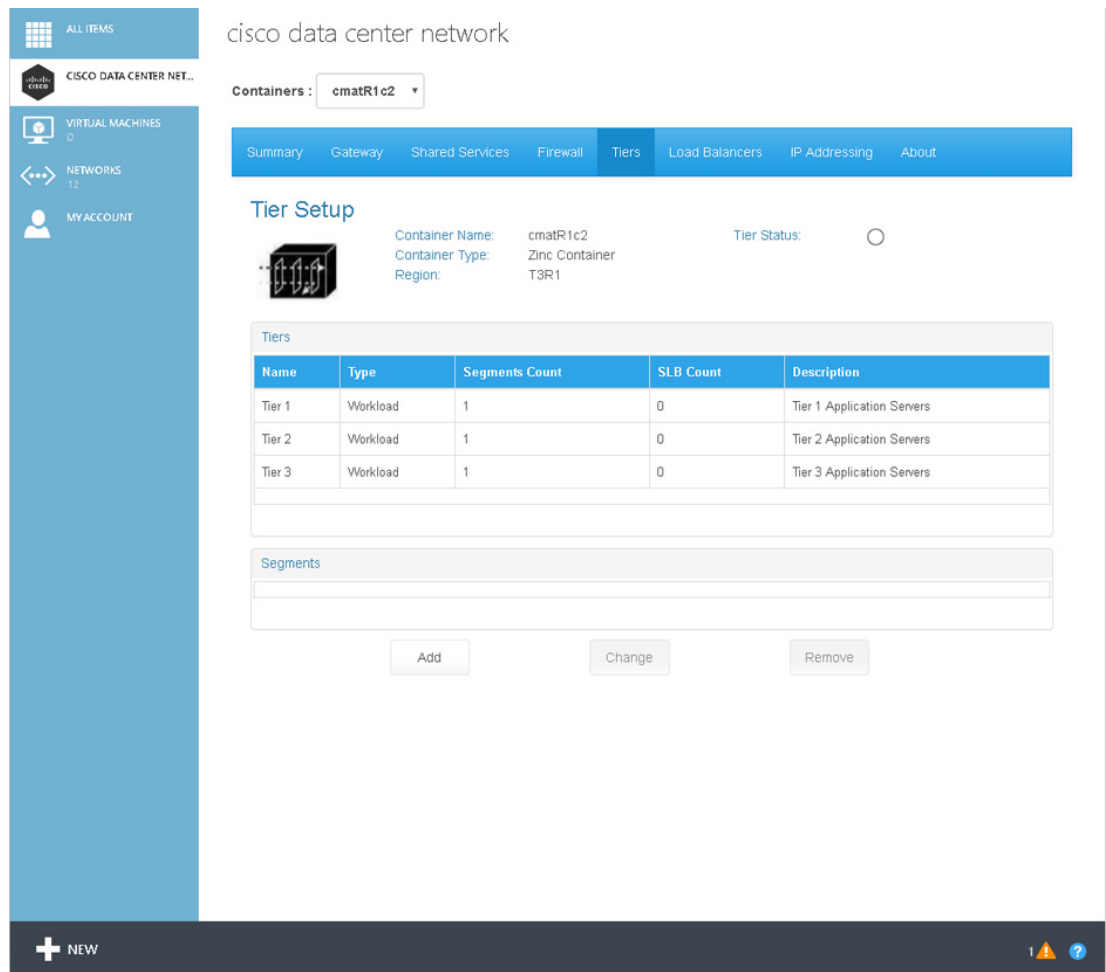
On the Tier tab, you can:

- Add a tier
- Change a tier, including update a segment
- Remove a tier
- Remove a segment

Step 1 To view tier information, click the **Tiers** tab.

You see the following screen.

Figure 2-49 Tiers Tab



The screenshot shows the Cisco Cloud Network Automation Provisioner interface. The left sidebar contains navigation options: ALL ITEMS, CISCO DATA CENTER NET..., VIRTUAL MACHINES (0), NETWORKS (12), and MYACCOUNT. The main content area is titled "cisco data center network" and shows a dropdown menu for "Containers" set to "cmatR1c2". Below this is a navigation bar with tabs: Summary, Gateway, Shared Services, Firewall, Tiers (selected), Load Balancers, IP Addressing, and About. The "Tier Setup" section displays the following information:

- Container Name: cmatR1c2
- Container Type: Zinc Container
- Region: T3R1
- Tier Status:

Below the tier setup information is a table titled "Tiers":

Name	Type	Segments Count	SLB Count	Description
Tier 1	Workload	1	0	Tier 1 Application Servers
Tier 2	Workload	1	0	Tier 2 Application Servers
Tier 3	Workload	1	0	Tier 3 Application Servers

Below the table is a section titled "Segments" with an empty list. At the bottom of the main content area are three buttons: Add, Change, and Remove. The bottom of the interface shows a "+ NEW" button and a status bar with a warning icon, a help icon, and the number "209995".

Step 2 To view segment information about a specific tier, click the tier name.

You see the following screen.

Figure 2-50 Tiers Screen—Tier Selected and Segment(s) Visible

The screenshot displays the 'Tiers Setup' page for a container named 'cmatR1c2'. The container is of type 'Zinc Container' and is located in the 'T3R1' region. The tier status is 'Online'. The page shows a list of tiers and a list of segments.

Name	Type	Segments Count	SLB Count	Description
Tier 1	Workload	1	0	Tier 1 Application Servers
Tier 2	Workload	1	0	Tier 2 Application Servers
Tier 3	Workload	1	0	Tier 3 Application Servers

Name	Network	Gateway	Description
Workload Segment 1	172.41.4.0/24	172.41.4.1	Segment 1 Description

The screen displays the following information:

- Container Name:—Displays the container name.
- Container Type:—Displays the container type instance name.
- Region:—Displays the Region name.
- Name:—Name of the tier.
- Description:—Description of the tier.
- Status:—Displays the Tiers status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
 - Green—Tier is Active.
 - Red—Tier is Inactive.
- Num Segments:—The number of segments in the tier.
- Tiers:
 - Name—Name given to the tier. The System assigns Tier *<space><number>* during container creation.
 - Type—It specifies the type of container to which the tier belongs.

- Num Segments—Tiers can contain multiple segments.
- Num SLB—Number of Server Load Balancers
- Description—A brief description of the tier (what the user intends to use it for, what services are hosted in it, etc.)
- Segments:
 - Name—Name given to the segment. The System assigns Segment *<space><number>* during container creation.
 - Network—The subnet address of this segment.
 - Gateway—The default gateway to access this segment.
 - Description—A brief description of the segment (what the user intends to use it for, what services are hosted in it, etc.).

Adding a Tier

To add a tier:

- Step 1** On the Tiers Tab screen, click **Add**.

You see the following screen.

Figure 2-51 Add a Tier Screen

The screen displays the following information:

- Type:—Workload and DMZ are supported in the current release.
- Name:—Enter a name for the tier.
- Description:—Enter a description for the tier.

- Enter L2 Segments—
 - Add—Add a segment. For more information, see the next section.
- L2 Segments—
 - Name—Name of the Layer 2 segment.
 - Sub Net—Subnet of the Layer 2 segment.
 - Description—Description of the Layer 2 segment.

Step 2 When you are finished, click **Add**.

Adding a Segment

When you are adding a tier, you must add a segment:

Step 1 On the Add Tier screen shown in the previous section, under Enter L2 Segments, click the addition symbol (+).

You see the following screen.

Figure 2-52 Add Segment Screen

The screenshot shows a modal dialog box titled "Add Segments" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Segment Information" which contains three input fields: "Name:", "Description:", and "Subnet:". The "Subnet:" field is pre-filled with the text "A.B.C.D/24". Below the input fields, there are two buttons: "Add" and "Close".

Enter information about the segment:

- Name—Name of the segment.
- Description—Description of the segment.
- Subnet—Subnet of the segment.

Step 2 When you are finished, click **Add**.

Changing a Tier

To change a tier:

Step 1 On the Tiers Tab screen, click the tier you want to change, then click **Change** (when you click a tier, you see segment information about the selected tier).

You see the following screen.

Figure 2-53 Change a Tier Screen

The screen displays the following information, some of which you can change:

- Tier Information:
 - Type:—Prepopulated
 - Name:—You can edit the name.
 - Description:—You can edit the description.
- L2 Segments—
 - Name—Name of the Layer 2 segment.
 - Description—Description of the Layer 2 segment.
 - Network—The network of the Layer 2 segment.

You can click a specific segment under L2 Segments to update it. For more information, see the next section.

Step 2 When you are finished, click **Change**.

Updating a Segment

When you are changing a tier, you can update a segment:

Step 1 On the Change Tier screen shown in the previous section, under L2 Segments, click the segment you want to update.

You see the following screen.

Figure 2-54 Update Segments Screen

The screenshot shows a web interface for updating an L2 segment. The title is "Change Segment". Below the title is a section labeled "L2 Segment". There are three input fields with labels: "*Name :", "*Subnet :", and "*Description :". The values entered in these fields are "Workload Segment 1", "A.B.C.D/24", and "Segment 1 Description" respectively.

You can change:

- Name:—You can edit the name of the segment
- Description:—You can edit the description of the segment.

Step 2 When you are finished, click **Update**.

You return to the previous screen.

Removing a Tier

To remove a tier, on the Tiers Tab screen, click the tier you want to remove, then click **Remove**. In the current release, you must return to the Tiers tab to force a reload and consequent fetch from the backend.

Mapping Public IP Addresses to Private DMZ IP Addresses

The DMZ tier is a perimeter network inside a container which is securely separated from the other interior networks of the container. The DMZ tier hosts applications and is accessible from the public Internet and other external networks having connectivity to the container edge.

To enable real-time inbound communication from the public Internet to your private cloud DMZ tier, your cloud provider can allow the servers you administer to be addressable on the public Internet. Your cloud provider can create pools of unallocated (unassigned) public IP addresses. Then, as needed, you can request that the cloud provider allocate (assign) these public IP addresses to you. You can map the allocated public IP addresses to private IP addresses within your DMZ tiers, including any DMZ Load Balancer VIP and any Workload VM addresses. Mapping directs inbound traffic from a public IP address to a private DMZ address. You can also unmap addresses.

For example, you might create a workload VM on the DMZ tier and want access to it from the Internet, in which case you request a public IP address from your cloud provider. You can then map the workload VM address to the public IP address you were allocated by the cloud provider.

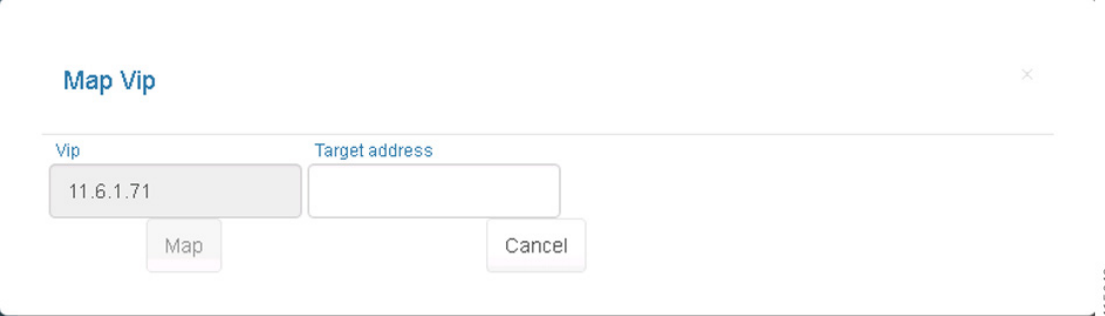
To view, map, and unmap IP addresses:

Step 1 Click the **IP Addressing** tab. You see the following screen.

Figure 2-55 IP Addressing Tab

The screenshot displays the 'IP Addressing' tab in the Cisco Cloud Network Automation Provisioner. The interface includes a left-hand navigation pane with 'ALL ITEMS', 'CISCO DATA CENTER NET...', and 'MYACCOUNT'. The main content area is titled 'cisco data center network' and features a 'Containers' dropdown menu set to 'cmat_mcsr_Container_1'. Below this is a horizontal navigation bar with tabs for 'Summary', 'Gateway', 'Shared Services', 'Firewall', 'Tiers', 'Load Balancers', 'IP Addressing', and 'About'. The 'IP Addressing' section is divided into two main areas: 'Unmapped Addresses' and 'Mapped Addresses'. The 'Unmapped Addresses' section contains a search bar labeled 'global search ...' and a list of five IP addresses: 11.6.1.71, 11.6.1.72, 11.6.1.73, 11.6.1.74, and 11.6.1.75. A 'Map To...' button is located below the list. The 'Mapped Addresses' section also has a search bar labeled 'global search ...' and an 'Unmap' button. At the bottom of the interface, there is a '+ NEW' button and a status bar with a warning icon, a list icon, a help icon, and the number '415047'.

Step 2 Click the IP address you want to map and click **Map To**. You see the following screen.

Figure 2-56 Map VIP

415049

Step 3 Enter the Target address and click **Map**.

Step 4 To unmap an IP address, click the mapped IP Address you want to unmap, then click **Unmap**. You see the following confirmation screen.

Figure 2-57 Unmap Confirmation

415162

Step 5 Click **Yes**.



APPENDIX A

Onboarding an Application from a Subscription

**Note**

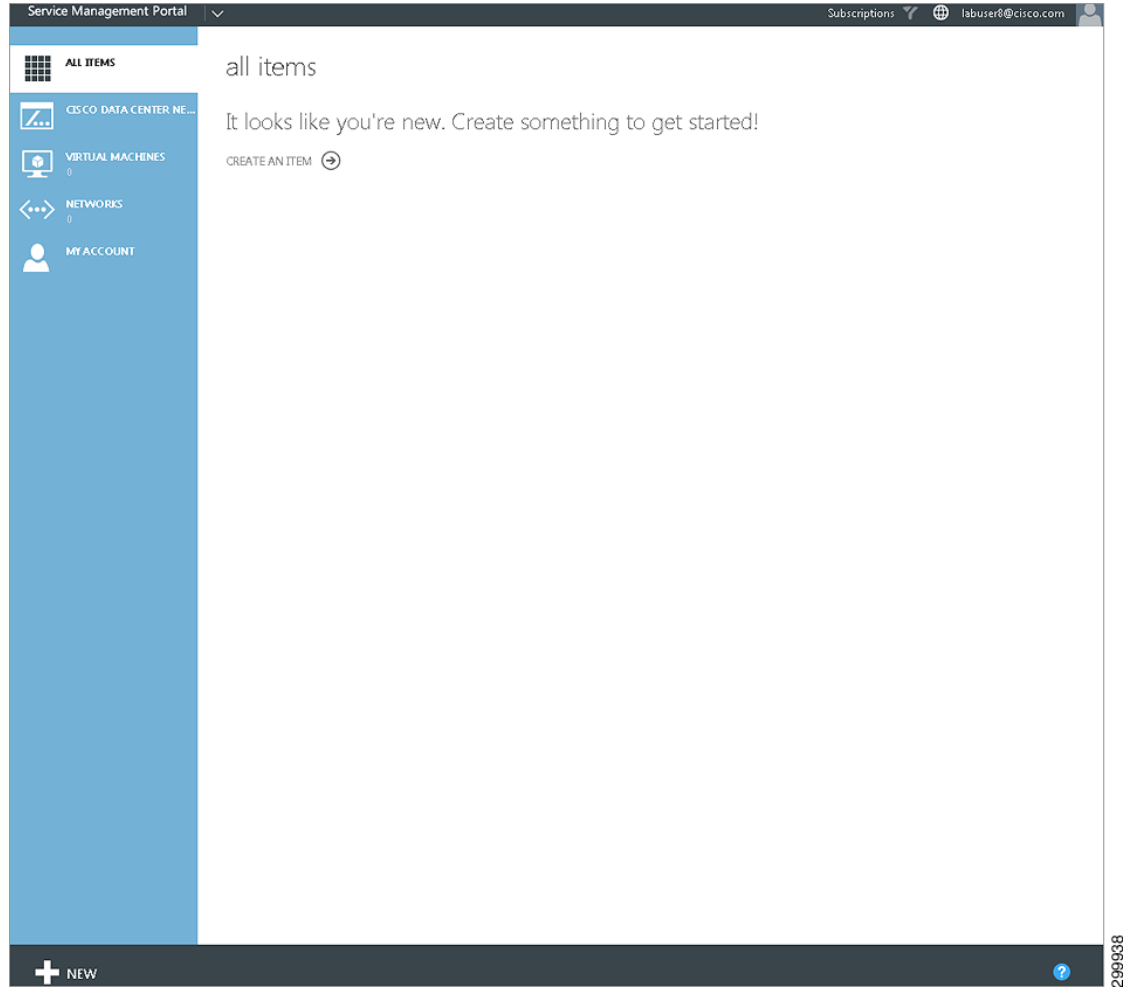
Use only standalone VM creation.

To onboard an application from a subscription:

Step 1 Subscribe to a plan with a network and Virtual Machine Cloud.

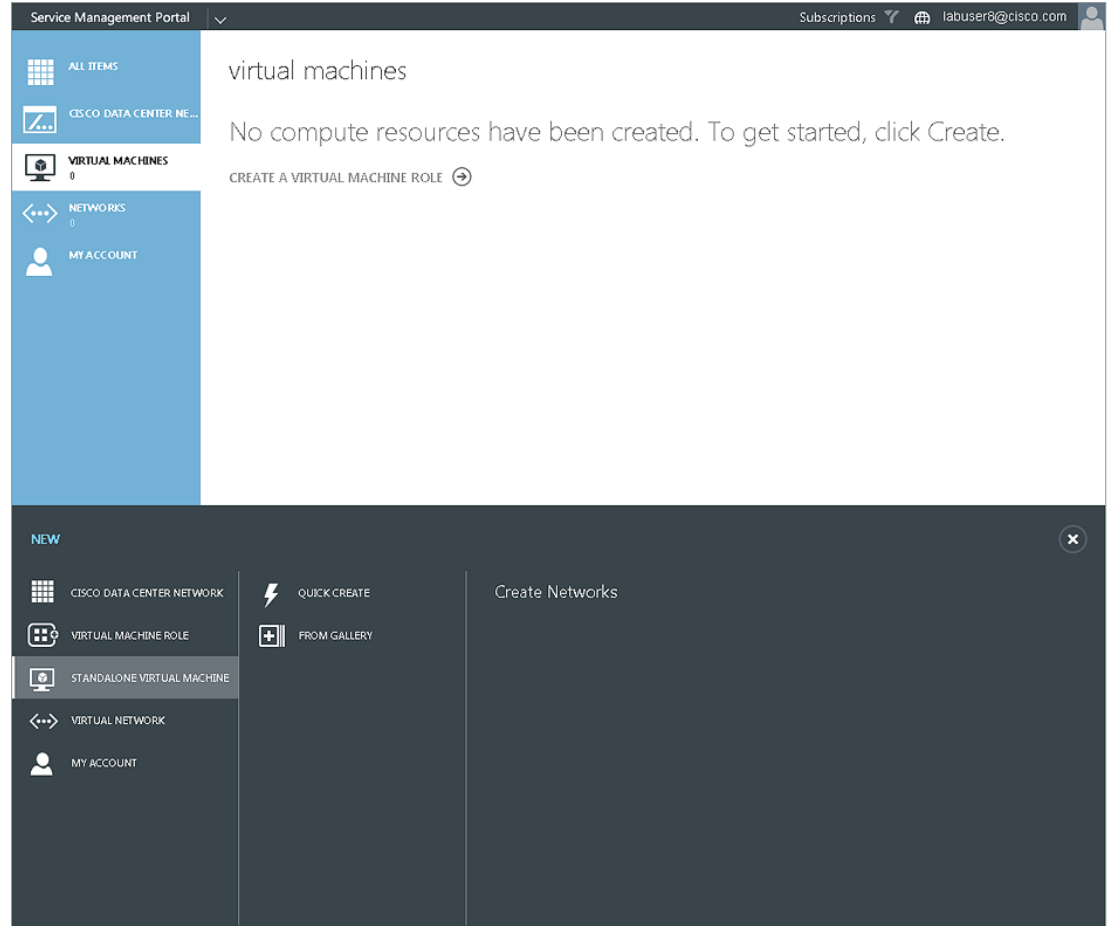
For information on subscribing to a plan, see [Subscribing to a Plan](#) in [Chapter 1, “Introduction.”](#) For information on the plans to which you can subscribe, contact your cloud provider.

On the main Tenant Portal screen you should see Virtual Machines in the left column, as shown in the following screen.

Figure A-1 Main Tenant Portal Screen

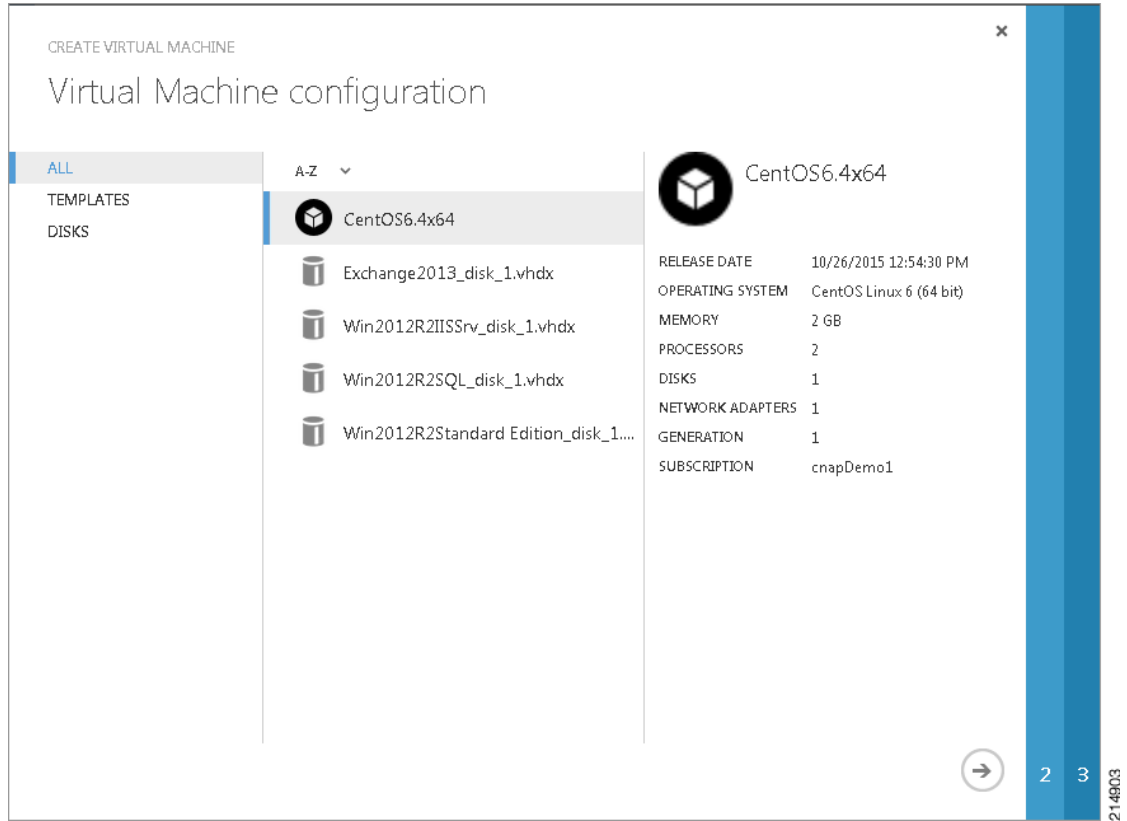
Step 2 Click + New, Standalone Virtual Machine, then From Gallery, as shown in the following screen.

Figure A-2 Create Virtual Machine Screen



You see the following screen.

Figure A-3 Virtual Machine Configuration



Step 3 In this example we selected **CentOS6.4x64**. Click the right arrow (→).
You see the following screen.

Figure A-4 Virtual Machine Settings

CREATE VIRTUAL MACHINE

Provide virtual machine settings

NAME

ADMINISTRATOR ACCOUNT

NEW PASSWORD

CONFIRM

ADMINISTRATOR SSH KEY

CentOS6.4x64

RELEASE DATE	10/26/2015 12:54:30 PM
OPERATING SYSTEM	CentOS Linux 6 (64 bit)
MEMORY	2 GB
PROCESSORS	2
DISKS	1
NETWORK ADAPTERS	1
GENERATION	1
SUBSCRIPTION	cnapDemo1

1 3 214904

Step 4 Enter a Name for the virtual machine, create a New Password, and Confirm it, as shown in the following screen.

Figure A-5 Name and Password Screen

CREATE VIRTUAL MACHINE

Provide virtual machine settings

NAME
Test Tier 1

ADMINISTRATOR ACCOUNT
root

NEW PASSWORD
●●●●●●●●

CONFIRM
●●●●●●●●

ADMINISTRATOR SSH KEY

CentOS6.4x64

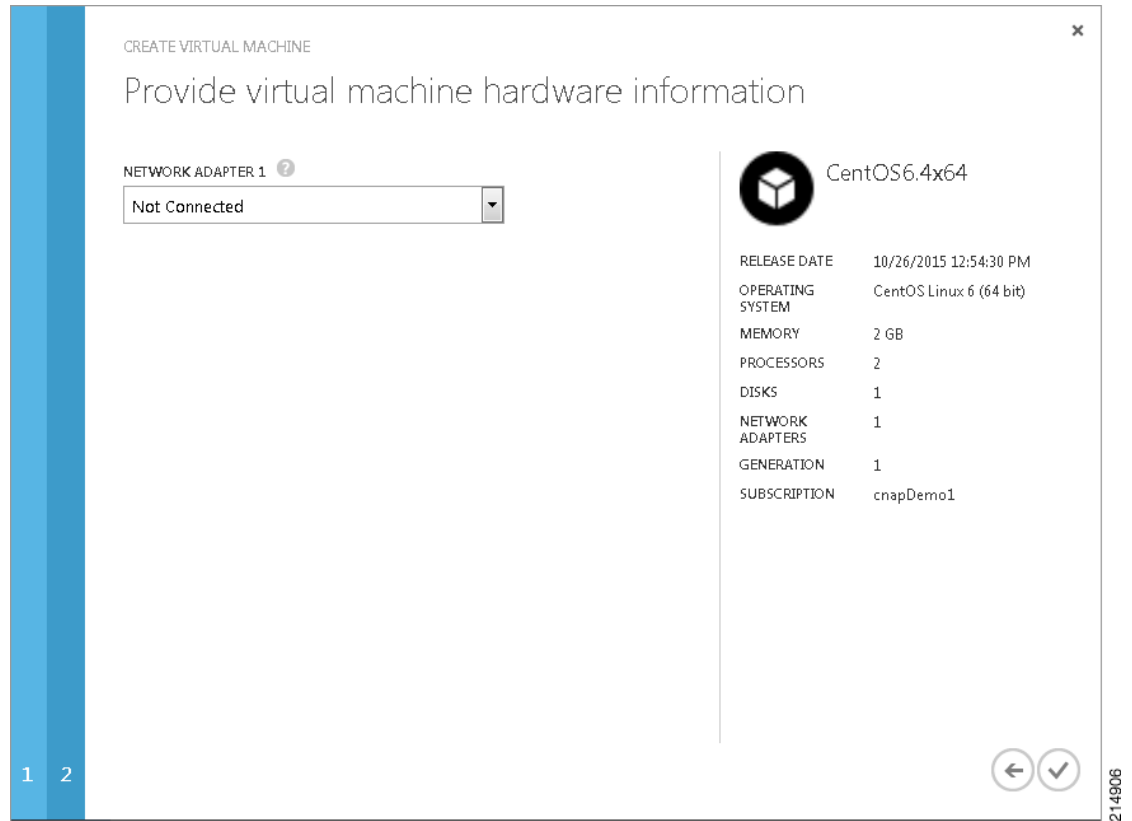
RELEASE DATE	10/26/2015 12:54:30 PM
OPERATING SYSTEM	CentOS Linux 6 (64 bit)
MEMORY	2 GB
PROCESSORS	2
DISKS	1
NETWORK ADAPTERS	1
GENERATION	1
SUBSCRIPTION	cnapDemo1

1

3

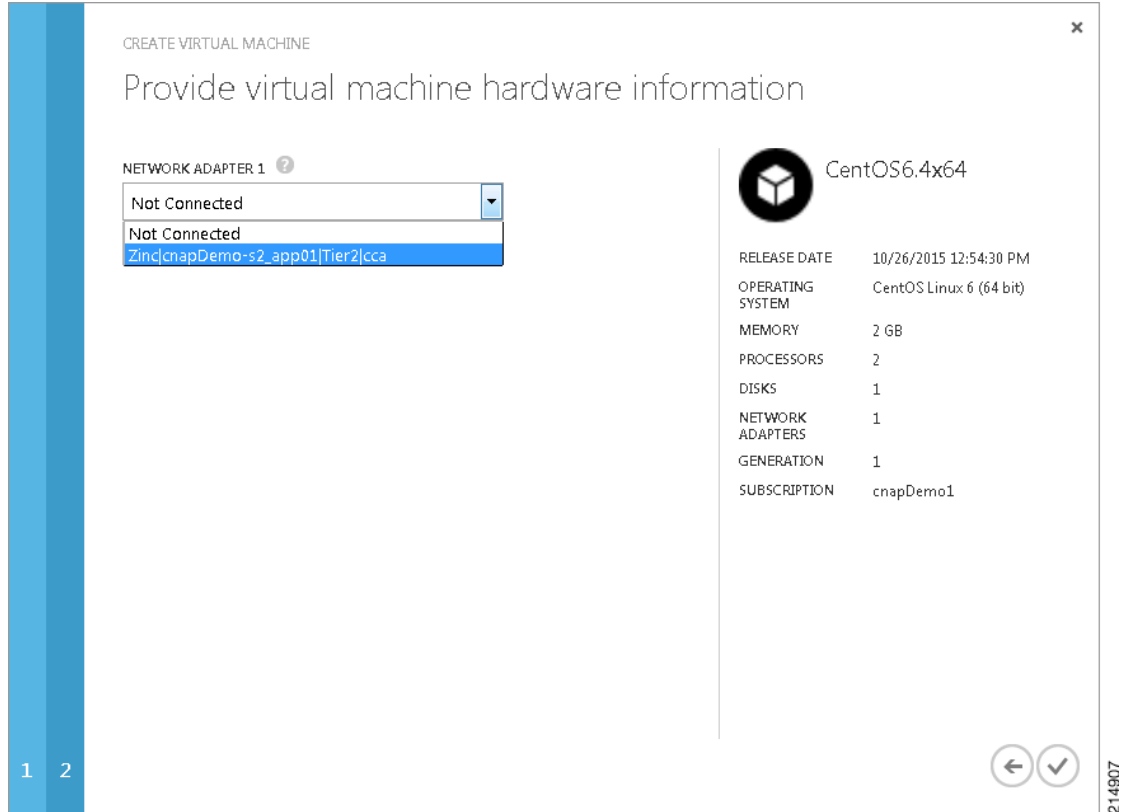
214905

- Step 5** Click the right arrow (→).
You see the following screen.

Figure A-6 Network Adapter Screen

Step 6 Select an adapter from the drop-down menu, as shown in the following screen.

Figure A-7 Network Adapter Selection



Step 7 Click the check mark.

You should be able to see your virtual machine being created from your dashboard, as shown in the following screen, where the virtual machine has a Status of Creating.

Figure A-8 Virtual Machine Creation in Process

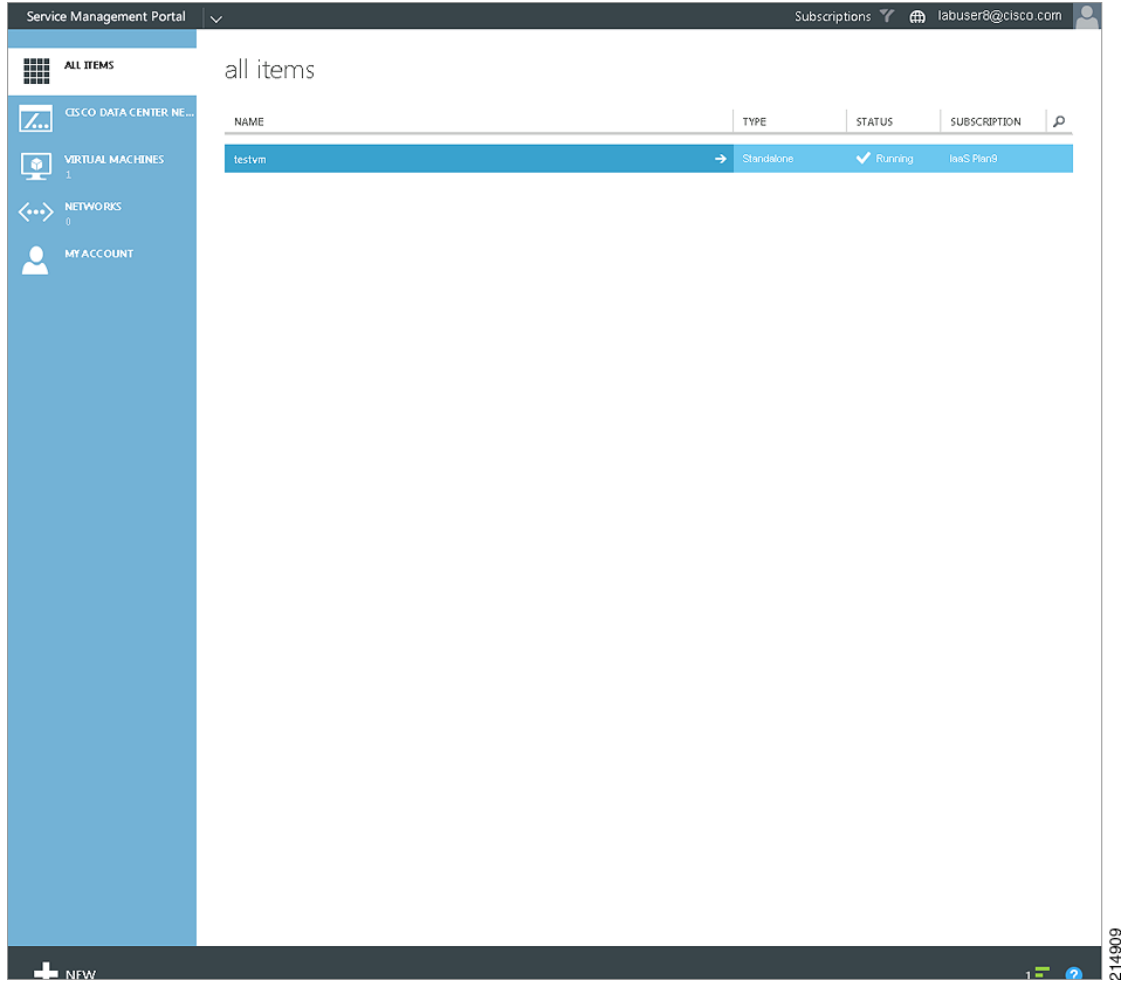
The screenshot displays the Service Management Portal interface. The top navigation bar includes 'Service Management Portal', 'Subscriptions', and the user 'labuser8@cisco.com'. A left sidebar contains navigation options: 'ALL ITEMS', 'CISCO DATA CENTER NE...', 'VIRTUAL MACHINES 1', 'NETWORKS 0', and 'MY ACCOUNT'. The main content area is titled 'all items' and features a table with the following structure:

NAME	TYPE	STATUS	SUBSCRIPTION
testvm	Standalone	Creating ..	iasS Plan9

At the bottom of the interface, there is a '+ NEW' button on the left and a notification icon with the number '1' on the right. A vertical ID '214908' is visible on the far right edge of the screenshot.

Virtual machine creation takes a few minutes as the virtual machine is created, boots, and is configured. When the virtual machine has been created, you see a screen like the following.

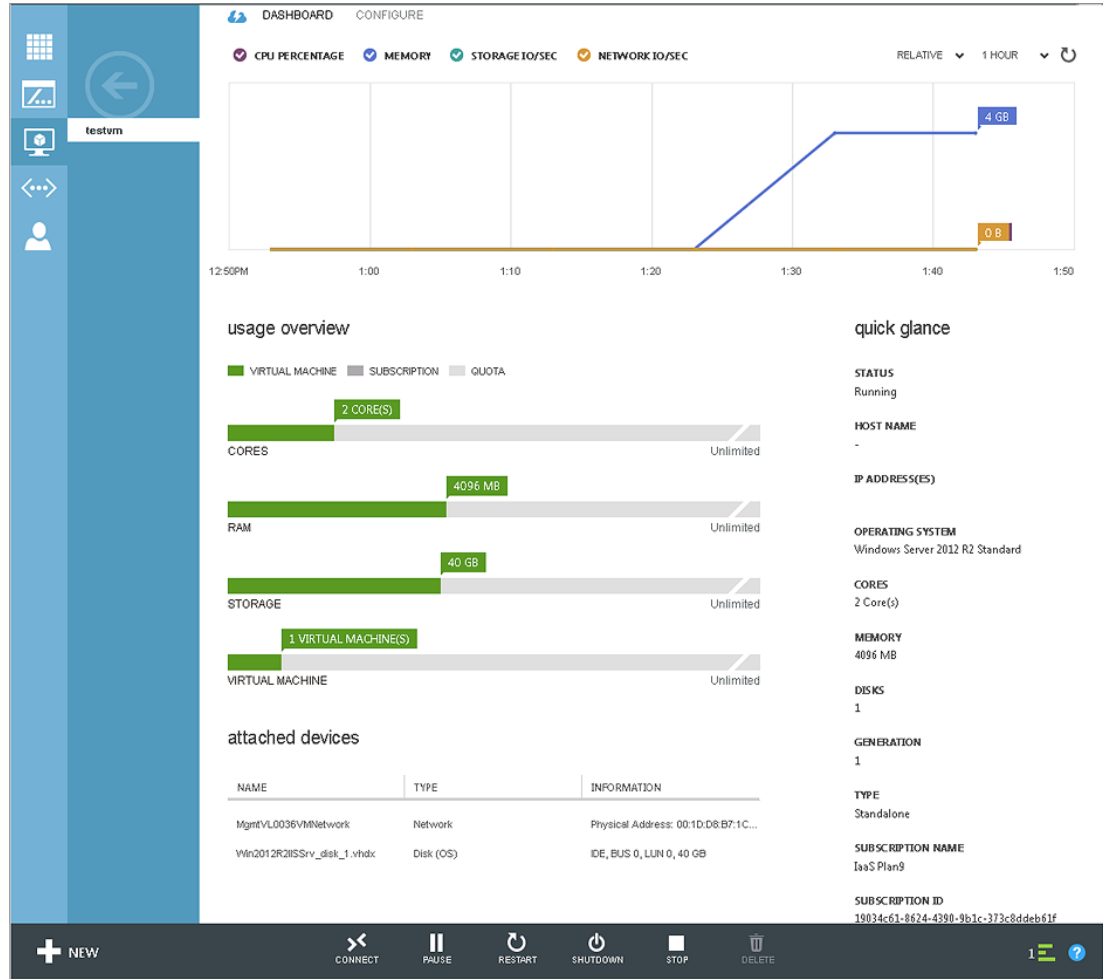
Figure A-9 Virtual Machine Created



Step 8 When creation is complete, the Status will change to Running. Click on the plan name, then click **Dashboard**.

You see the following screen, which shows you information about your virtual machine.

Figure A-10 Virtual Machine Information



214910

