Cisco Virtual Network Management Center 2.1 GUI Configuration Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28663-01

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Google, Google Play, Android and certain other marks are trademarks of Google Inc.

© 2012-2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xiii

Audience xiii

Organization xiii

Conventions xiv

Related Documentation xv

Documentation Feedback xvi

Obtaining Documentation and Submitting a Service Request xvi

CHAPTER 1

Overview 1

CHAPTER 2

Overview of the VNMC GUI 5

Firewall Access 5

Login URL 6

User Interface Components 6

Toolbar 8

Field Aids 8

Inactivity Timeout Period 9

Changes with VNMC Installed on Microsoft Hyper-V Server 2012 (Hyper-V Hypervisor) 9

Search 10

Clone 11

CHAPTER 3

Configuring Primary Authentication 13

Primary Authentication 13

Remote Authentication Providers 13

Creating an LDAP Provider 14

Editing an LDAP Provider 16

Deleting an LDAP Provider 17

Selecting a Primary Authentication Service 17

CHAPTER 4 Configuring RBAC 19

RBAC 19

User Accounts 19

Username Guidelines 20

Password Guidelines 20

User Roles 21

Privileges 22

User Locales 23

Configuring User Roles 24

Creating a User Role 24

Editing a User Role 25

Deleting a User Role 25

Configuring User Locales 26

Creating a Locale 26

Editing a Locale 27

Deleting a Locale 27

Assigning an Organization to a Locale 28

Deleting an Organization from a Locale 28

Configuring Locally Authenticated User Accounts 28

Creating a User Account 28

Changing the Locales or Roles Assigned to a Locally Authenticated User 32

Changing the Roles Assigned to a Locally Authenticated User Account 32

Monitoring User Sessions 32

CHAPTER 5 Configuring Trusted Points 35

Trusted Points 35

Configuring Trusted Points 35

Creating a Trusted Point 35

Editing a Trusted Point 36

Deleting a Trusted Point 36

CHAPTER 6 Configuring VNMC Profiles 37

Profiles 37

Policies in VNMC Profiles 37
Configuring Policies 38
Configuring a Core File Policy 38
Adding a Core File Policy to the VNMC Profile 38
Editing a Core File Policy for a VNMC Profile 39
Deleting a Core File Policy from the VNMC Profile 40
Configuring a Fault Policy 40
Adding a Fault Policy to the VNMC Profile 40
Editing a Fault Policy for a VNMC Profile 41
Deleting a Fault Policy from the VNMC Profile 43
Configuring a Logging Policy 43
Adding a Logging Policy to the VNMC Profile 43
Editing a Logging Policy for VNMC Profile 44
Deleting a Logging Policy from the VNMC Profile 45
Configuring a Syslog Policy 46
Adding a Syslog Policy to the VNMC Profile 46
Editing a Syslog Policy for the VNMC Profile 48
Deleting a Syslog Policy from a VNMC Profile 51
Adding a Syslog Server to the VNMC Profile 52
Editing a Syslog Server for the VNMC Profile 54
Deleting a Syslog Server from a VNMC Profile 56
Configuring the Default Profile 56
Editing the VNMC Default Profile 56
Configuring a DNS Server 59
Adding a DNS Server 59
Deleting a DNS Server 59
Configuring an NTP Server 59
Adding an NTP Server 59
Deleting an NTP Server 60
Configuring a DNS Domain 60
Editing a DNS Domain 60

CHAPTER 7 **Configuring VM Managers 61**
VM Manager Overview 61
Configuring VM Managers Under Administration 62

Adding a VM Manager Under Administration 62
Editing a VM Manager 63
Deleting a VM Manager 64
Configuring VM Managers Under Resource Management 64
Adding a VM Manager Under Resource Management 64
Editing a VM Manager 65
Deleting a VM Manager 67

CHAPTER 8 Configuring Tenants 69
Tenant Management 69
Tenant Management and Multi-Tenant Environments 69
Name Resolution in a Multi-Tenant Environment 70
Configuring Tenants 70
Creating a Tenant 70
Editing a Tenant 71
Deleting a Tenant 71
Configuring Virtual Data Centers 72
Creating a Virtual Data Center 72
Editing a Virtual Data Center 72
Deleting a Virtual Data Center 73
Configuring Applications 73
Creating an Application 73
Editing an Application 74
Deleting an Application 74
Configuring Tiers 74
Creating a Tier 74
Editing a Tier 75
Deleting a Tier 75

CHAPTER 9 Configuring Service Policies and Profiles 77
Configuring Service Policies 77
Configuring ACL Policies and Policy Sets 77
Adding an ACL Policy 78
Add ACL Policy Rule Dialog Box 78
Time Ranges in ACL Policy Rules 82

Adding an ACL Policy Set 84
Configuring Connection Timeout Policies 84
Add Connection Timeout Policy Rule Dialog Box 85
Configuring DHCP Policies 86
Adding a DHCP Relay Server 86
Add DHCP Relay Server Dialog Box 87
Configuring a DHCP Relay Policy 87
Add DHCP Relay Policy Dialog Box 87
Configuring a DHCP Server Policy 88
Add DHCP Server Policy Dialog Box 88
Configuring IP Audit and IP Audit Signature Policies 89
Configuring IP Audit Policies 90
Add IP Audit Policy Rule Dialog Box 90
Configuring IP Audit Signature Policies 91
Configuring NAT/PAT Policies and Policy Sets 92
Configuring NAT/PAT Policies 92
Add NAT Policy Rule Dialog Box 93
Add NAT Policy Rule Dialog Box 93
Configuring NAT Policy Sets 95
Configuring PAT for Edge Firewalls 95
Configuring Source Dynamic Interface PAT 96
Configuring Destination Static Interface PAT 96
Configuring Packet Inspection Policies 97
Protocols Supported for Packet Inspection Policies 97
Add Packet Inspection Policy Rule Dialog Box 98
Configuring Routing Policies 98
Configuring TCP Intercept Policies 99
Add TCP Intercept Policy Rule Dialog Box 99
Configuring Site-to-Site IPsec VPN Policies 100
Configuring Crypto Map Policies 100
Add Crypto Map Policy Dialog Box 101
Add Crypto Map Policy Rule Dialog Box 103
Configuring IKE Policies 103
IKE V1 Policy Dialog Box 104
IKE V2 Policy Dialog Box 104

Configuring Interface Policy Sets 105
Add Interface Policy Set Dialog Box 105
Configuring IPsec Policies 106
IPsec IKEv1 Proposal Dialog Box 107
IPsec IKEv2 Proposal Dialog Box 108
Configuring Peer Authentication Policies 109
Add Policy to Authenticate Peer Dialog Box 109
Configuring VPN Device Policies 110
Add VPN Device Policy Dialog Box 111
Working with Profiles 113
Configuring Compute Security Profiles 113
Add Compute Security Profile Dialog Box 114
Verifying Compute Firewall Policies 115
Configuring Edge Device Profiles 115
Edge Device Profile Dialog Box 116
Configuring Edge Security Profiles 117
Add Edge Security Profile Dialog Box 118
Applying an Edge Device Profile 119
Applying an Edge Security Profile 120
Verifying Edge Firewall Policies 120
Configuring Security Profiles 121
Editing a Security Profile for a Compute Firewall 121
Editing a Security Profile for an Edge Firewall 122
Deleting a Security Profile 124
Deleting a Security Profile Attribute 124
Assigning a Policy 125
Unassigning a Policy 125
Configuring Security Policy Attributes 125
Configuring Object Groups 125
Adding an Object Group 125
Adding an Object Group Expression 126
Editing an Object Group 127
Editing an Object Group Expression 128
Deleting an Object Group 128
Deleting an Object Group Expression 129

Configuring Security Profile Dictionary 129
Adding a Security Profile Dictionary 129
Adding a Security Profile Dictionary Attribute 130
Editing a Security Profile Dictionary 131
Editing a Security Profile Dictionary Attribute 131
Deleting a Security Profile Dictionary 132
Deleting a Security Profile Dictionary Attribute 132
Working with vZones 132
Adding a vZone 133
Editing a vZone 134
Deleting a vZone Condition 135
Deleting a vZone 135

CHAPTER 10 **Configuring Device Policies and Profiles 137**
Device Policies and Profiles 137
Device Profiles 137
Policies 138
Device Configuration 138
Device Policies 139
Configuring Device Policies 139
Configuring AAA Policies 139
Field Descriptions 140
Add Auth Policy Dialog Box 140
Remote Access Method Dialog Box 141
Configuring Core File Policies 142
Adding a Core File Policy for a Device 142
Editing a Core File Policy for a Device Profile 143
Deleting a Core File Policy from a Device Profile 143
Configuring Fault Policies 144
Adding a Fault Policy for a Device Profile 144
Editing a Fault Policy for a Device Profile 145
Deleting a Fault Policy for a Device Profile 146
Configuring Log File Policies 147
Adding a Logging Policy for a Device Profile 147
Editing a Logging Policy for a Device Profile 148

Deleting a Logging Policy for a Device Profile 149
Configuring SNMP Policies 150
Adding an SNMP Policy 150
Editing an SNMP Policy 151
Deleting an SNMP Policy 152
Adding an SNMP Trap Receiver 153
Editing an SNMP Trap Receiver 153
Deleting an SNMP Trap Receiver 154
Configuring Syslog Policies 154
Adding a Syslog Policy for a Device 154
Field Descriptions 154
Add Syslog Policy Dialog Box 154
Editing a Syslog Policy for a Device Profile 157
Deleting a Syslog Policy for a Device Profile 160
Adding a Syslog Server for a Device Profile 160
Field Descriptions 160
Add Syslog Server Dialog Box 160
Editing a Syslog Server for a Device Profile 163
Deleting a Syslog Server for a Device Profile 165
Configuring Device Profiles 165
Adding a Firewall Device Profile 165
Editing a Firewall Device Profile 167
Deleting a Firewall Device Profile 170
Configuring NTP 170
Creating a Device Profile with NTP 170
Field Descriptions 171
Add NTP Server Dialog Box 171
Applying Device Profiles to Compute Firewalls 172
Applying Device Profiles to Edge Firewalls 172
Associating Device Policies with Profiles 172

CHAPTER 11 **Configuring Managed Resources** 175
Resource Management 175
Resource Manager 176
Virtual Machines 176

Virtual Security Gateways 176
ASA 1000V Cloud Firewalls 177
Managing Compute Firewalls 177
Adding a Compute Firewall 177
Editing a Compute Firewall 178
Deleting a Compute Firewall 181
Assigning a VSG 181
Unassigning a VSG 182
Managing Edge Firewalls 182
Adding an Edge Firewall 182
Add Edge Firewall Dialog Box 183
Adding a Data Interface 183
Add Data Interface Dialog Box 183
Assigning an ASA 1000V 184
Unassigning an ASA 1000V 185
Verifying VM Registration in VNMC 185
Examining Fault Details 185
Examining Faults and Configuration Errors for Edge Firewalls 186
Examining Faults for Compute Firewalls 186
Launching ASDM from VNMC 187
Example Screens for ASDM 189
Managing Pools 190
Adding a Pool 190
Assigning a Pool 191
Editing a Pool 191
Unassigning a Pool 192
Deleting a Pool 192

CHAPTER 12 **Configuring Administrative Operations** 193
Administrative Operation Conventions 193
Managing Backup Operations 193
Creating a Backup Operation 194
Running a Backup Operation 195
Editing a Backup Operation 196
Deleting a Backup Operation 198

Restoring a Backup Configuration 198
Managing Export Operations 200
Creating an Export Operation 200
Editing an Export Operation 202
Deleting an Export Operation 203
Configuring Import Operations 204
Creating an Import Operation 204
Editing an Import Operation 205
Deleting an Import Operation 207

Preface

This preface includes the following sections:

- Audience, page xiii
- Organization, page xiii
- Conventions, page xiv
- Related Documentation, page xv
- Documentation Feedback, page xvi
- Obtaining Documentation and Submitting a Service Request, page xvi

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following areas:

- Server administration
- Storage administration
- Network administration
- Network security

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview	Contains an overview of Cisco Virtual Network Management Center (VNMC).
Chapter 2	Overview of the VNMC GUI	Contains an overview of the VNMC UI.

Chapter	Title	Description
Chapter 3	Configuring Primary Authentication	Describes how to configure LDAP providers and select a primary authentication service.
Chapter 4	Configuring RBAC	Describes how to configure role-based access control including user locales, user roles, and locally authenticated user accounts. This chapter also describes how to monitor user sessions.
Chapter 5	Configuring Trusted Points	Describes how to configure trusted points.
Chapter 6	Configuring VNMC Profiles	Describes how to configure VNMC policies and profiles.
Chapter 7	Configuring VNMC Managers	Describes how to configure VM Managers.
Chapter 8	Configuring Tenants	Describes how to configure tenants, data centers, applications, and tiers.
Chapter 9	Configuring Service Policies and Profiles	Describes how to configure service policies and policy sets, verify policies, configure compute and edge firewall security policies, and apply profiles to firewalls.
Chapter 10	Configuring Device Policies and Profiles	Describes how to configure device policies and device profiles, and associate device policies with profiles.
Chapter 11	Configuring Managed Resources	Describes how to configure managed resources including compute and edge firewalls, and pools.
Chapter 12	Configuring Administrative Operations	Describes how to configure backup operations, export operations, and import operations.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.

Convention	Indication
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
`Courier` font	Terminal sessions and information that the system displays appear in `Courier` font.
`Bold Courier` font	Information that you enter appears in **`bold Courier`** font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

Cisco Virtual Network Management Center

The following Cisco Virtual Network Management Center documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

- *Cisco Virtual Network Management Center 2.1 Documentation Overview*
- *Cisco Virtual Network Management Center 2.1 Release Notes*
- *Cisco Virtual Network Management Center 2.1 Quick Start Guide*

- *Cisco Virtual Network Management Center 2.1 CLI Configuration Guide*
- *Cisco Virtual Network Management Center 2.1 GUI Configuration Guide*
- *Cisco Virtual Network Management Center 2.1 XML API Reference Guide*
- *Open Source Used in Cisco Virtual Network Management Center 2.1*

Cisco ASA 1000V Documentation

The Cisco Adaptive Security Appliance (ASA) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

Cisco Virtual Security Gateway Documentation

The Cisco Virtual Security Gateway (VSG) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Documentation Feedback

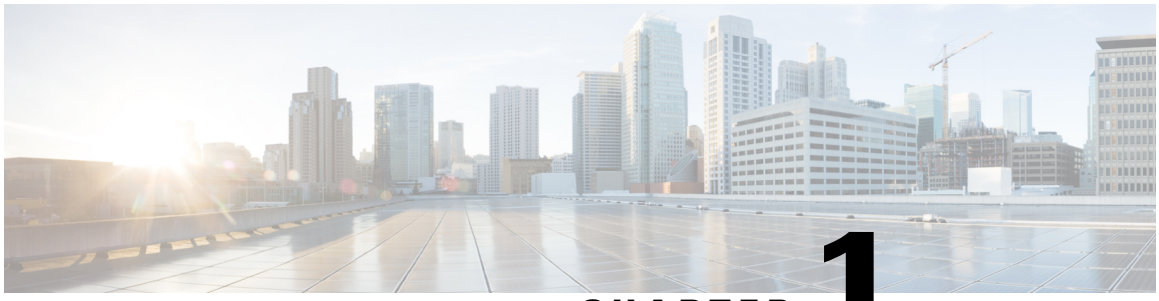
To provide technical feedback on this document, or to report an error or omission, please send your comments to vnmc-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Overview

Cisco Virtual Network Management Center (VNMC) is a virtual appliance, based on Red Hat Enterprise Linux, that provides centralized device and security policy management of Cisco virtual services. Designed for multi-tenant operation, VNMC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. With both a built-in GUI and an XML API, VNMC enables centralized management of Cisco virtual services by an administrator or programmatically.

VNMC is built on an information model-driven architecture in which each managed device is represented by its subcomponents (or *objects*), which are parametrically defined. This model-centric approach enables VNMC to provide a secure, multi-tenant virtualized infrastructure with Cisco Adaptive Security Appliance 1000V (ASA 1000V) and Cisco Virtual Security Gateway (VSG) virtual services.

The following table describes the primary features of VNMC.

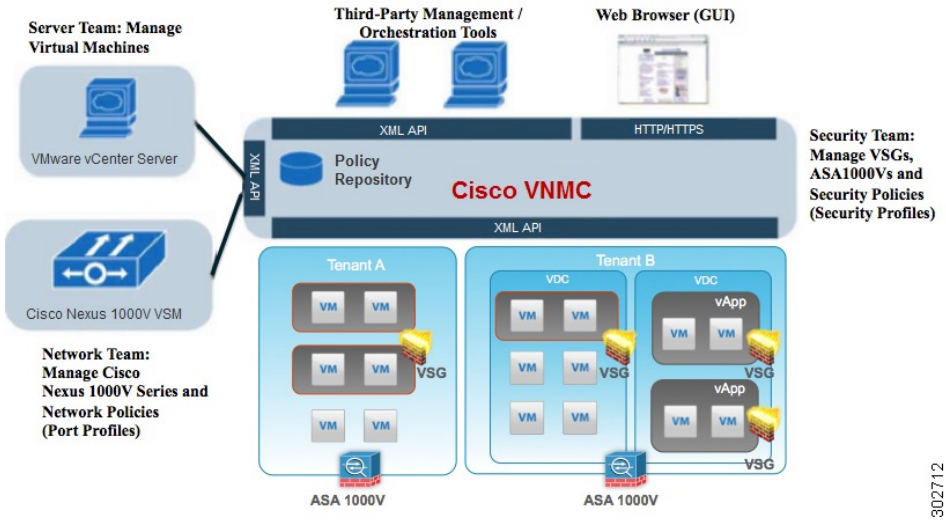
Table 1: VNMC 2.1 Features

Feature	Description
Multiple-Device Management	All ASA 1000Vs and VSGs are centrally managed, thereby simplifying provisioning and troubleshooting in a scaled-out data center. By using device profiles with their specified device configuration policies, you can deploy consistent policies to one or more profile-managed resources.
Security Profiles	Security profiles enable you to represent a security policy configuration in a profile that: • Simplifies provisioning • Reduces administrative errors during security policy changes • Reduces audit complexities • Enables a highly scaled-out data center environment

Feature	Description
Stateless Device Provisioning	The management agents in VSG and ASA 1000V are stateless, receiving information from VNMC and thereby enhancing scalability.
Security Policy Management	Security policies are authored, edited, and provisioned for all VSGs and ASA 1000Vs in a data center, which simplifies the operation and management of security policies, and ensures that the required security is accurately represented in the associated security policies.
Context-Aware Security Policies	VNMC interacts with VMware vCenter to create virtual machine (VM) contexts that enable you to institute highly specific policy controls across the entire virtual infrastructure.
Dynamic Security Policy and Zone Provisioning	VNMC interacts with the Cisco Nexus 1000V Virtual Supervisor Module (VSM) to bind the security profile with the corresponding Cisco Nexus 1000V Series switch port profile. When VMs are dynamically instantiated and applied to appropriate port profiles, their association to trust zones is also established.
Multi-Tenant Management	VNMC can manage compute and edge firewall security policies in a dense multi-tenant environment, so that you can rapidly add or delete tenants, and update tenant-specific configurations and security policies. This feature significantly reduces administrative errors, ensures segregation of duties within the administrative team, and simplifies audit procedures.
Role-Based Access Control	Role-Based Access Control (RBAC) simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures. This support reduces administrative errors, enables detailed control of user privileges, and simplifies auditing requirements.
XML-Based API	The VNMC XML application programming interface (API) allows external system management and orchestration tools to programmatically provision VSGs and ASA 1000Vs, and provides transparent and scalable operation management.

The following figure illustrates how VNMC relates to other components in a multi-tenant environment, including virtual machines, virtual services, and user and programmatic interfaces.

Figure 1: VNMC in a Multi-Tenant Environment



VNMC provides centralized device and policy management of VSGs and ASA 1000Vs in multi-tenant virtual data centers and private or public clouds.

VNMC uses security profiles for template-based configuration of security policies. A security profile is a collection of security policies that can be predefined and applied on an on-demand basis at the time of VM instantiation. This profile-based approach significantly simplifies authoring, deployment, and management of security policies in a dense multi-tenant environment while enhancing deployment agility and scaling. Security profiles also help reduce administrative errors and simplify audits.

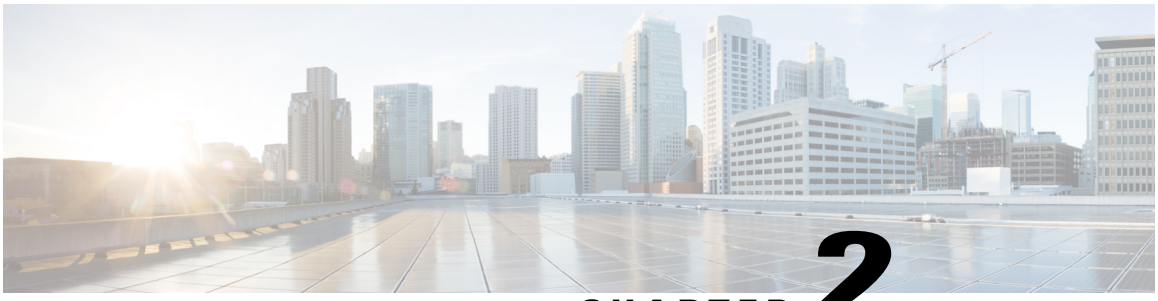
The VNMC XML API facilitates coordination with third-party provisioning tools for programmatic provisioning and management of VSGs and ASA 1000Vs.

By providing visual and programmatic controls, VNMC enables the security operations team to author and manage security policies for the virtualized infrastructure, and enhances collaboration with server and network operations teams. This administration model helps ensure the administrative segregation of duties to minimize administrative errors and to simplify regulatory compliance and auditing. For example, by using VNMC with the Cisco Nexus 1000V series VSM in your environment, your staff could align operations and responsibilities as follows:

- Security administrators—Author and manage security profiles, and manage VSG and ASA 1000V instances.
- Network administrators—Author and manage port profiles and manage Cisco Nexus 1000V Series switches. Port profiles with referenced security profiles are available in VMware vCenter through the Nexus 1000V VSM's programmatic interface with VMware vCenter.
- Server administrators—Select the appropriate port profile in VMware vCenter when instantiating a virtual machine.

VNMC implements an information model-driven architecture in which each managed device, such as an ASA 1000V or VSG, is represented by the object-information model of the device. Specifically, this model-driven architecture helps enable the use of:

- Stateless managed devices—Security policies and object configurations are abstracted into a centralized repository.
- Dynamic device allocation—A centralized resource management function manages pools of devices that are commissioned and a pool of devices that are available for commissioning. This approach simplifies large-scale deployments because managed devices can be preinstantiated and then configured on demand. In addition, devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools.
- Scalable management—A distributed management-plane function is implemented by using an embedded management agent on each managed device, thereby enabling greater scalability.



CHAPTER 2

Overview of the VNMC GUI

VNMC provides a browser-based interface that enables you to configure managed endpoints, perform administrative operational tasks, and define and apply policies and profiles. You can also use the GUI to manage and provision compute and edge firewalls, such as VSGs and ASA 1000Vs.

The following topics provide an overview of the VNMC user interface.

- Firewall Access, page 5
- Login URL, page 6
- User Interface Components, page 6
- Toolbar, page 8
- Field Aids, page 8
- Inactivity Timeout Period, page 9
- Changes with VNMC Installed on Microsoft Hyper-V Server 2012 (Hyper-V Hypervisor), page 9
- Search, page 10
- Clone, page 11

Firewall Access

If the VNMC server is protected by a firewall, the following ports must be enabled:

- 80—HTTP
- 443—HTTPS
- 843—Adobe Flash

Login URL

The default HTTPS URL for logging into the VNMC user interface is https://*server-ip-address*, where *server-ip-address* is the IP address assigned to the VNMC server. The IP address is the address for the management port.

Note If you log in using HTTP, you are automatically redirected to the HTTPS link.

User Interface Components

When you log into VNMC, the user interface is displayed.

The VNMC user interface contains the components described in the following table:

Table 2: VNMC User Interface Components

Component	Description
Title	Displays "Cisco Virtual Network Management Center."
Toolbar	Allows you to set inactivity timeout values, obtain product version information, access online help, and provide product feedback.
Tabs	Provide access to the primary VNMC components for managing your environment: • Tenant Management • Resource Management • Policy Management • Administration
Navigation pane	Provides navigation to all objects in the VNMC instance. The navigation pane is displayed on the left side of the screen below the tabs. The objects that are displayed in the navigation pane depend on the selected tab.
Content pane	Displays information and provides options for the object that is selected in the navigation pane.

The following table provides information about the tabs in the VNMC GUI:

Table 3: Tabs in the VNMC GUI

Tab	Description
Tenant Management	Enables you to manage tenants in the current VNMC instance. A system or server administrator can use this tab to create organizational hierarchies and enable multi-tenant management domains. The organizational hierarchy levels are Tenant > Virtual Data Center > Application > Tier.
Resource Management	Enables you to manage logical resources, such as VSGs, ASA 1000Vs, VSGs, and vCenters. Resource Management subtabs are: • Managed Resources • Resources • Capabilities • Diagnostics
Policy Management	Enables you to configure service and device policies and profiles, and to assign policies to profiles. Policy Management subtabs are: • Service Profiles • Service Policies • Device Configurations • Capabilities • Diagnostics
Administration	Provides the tools needed for administering VNMC. Administration subtabs are: • Access Control • Service Registry • VNMC Profile • VM Managers • Diagnostics • Operations

Toolbar

The VNMC toolbar displays in the upper-right portion of the user interface. The following table describes the toolbar options:

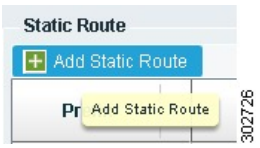
Table 4: Toolbar Options

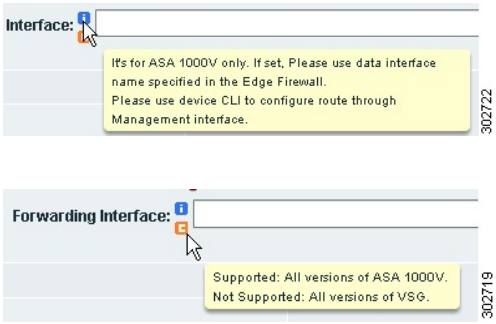
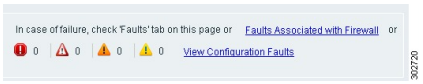
Option	Description
(*username*)	Username of the current VNMC session.
Preferences	Enables you to specify the amount of time that the VNMC session can remain inactive before the session times out. The value that you specify applies to the system from which you logged into VNMC.
Log Out	Logs you out of the current session.
About	Provides VNMC version information.
Help	Launches online help for the currently displayed screen.
Feedback	Allows you to provide feedback on VNMC.

Field Aids

VNMC includes the following aids to assist you in your tasks, whether configuring policies and profiles, troubleshooting faults, or looking for additional information for a particular window or dialog box.

Table 5: VNMC Field Aids

Feature	Description	Example
Tooltips	Pause your cursor over a field to view additional information about the field.	
Red field or box	Indicates that information is required. If you have entered information and the field remains red, the entry contains an error (such as an incomplete IP address). You can pause your mouse over the field to obtain information about the error.	

Feature	Description	Example
Field icons	Two field icons (i and c) provide additional information for the field: • The "i" icon provides additional information for the field. • The "c" icon identifies the feature support for the field. For example, a feature might be supported on ASA 1000Vs but not on VSGs. Pause your cursor over the icon to view the information.	
Fault links	Fault information and links to fault information are available for each edge and compute firewall in Resource Management. Navigate to a specific compute or edge firewall to view the object state, number of faults, and severity of faults. The same pane provides links to the relevant fault page.	
Online help	Context-sensitive online help is available for each VNMC pane and dialog box. To access help, click **Help** in the active pane or **?** in the active dialog box.	

Inactivity Timeout Period

The Preferences dialog box allows you to specify the length of time, from 5 to 60 minutes, that a VNMC session on your current machine can remain inactive before the session is closed. The value that you enter applies to the system that you used to log into VNMC.

Changes with VNMC Installed on Microsoft Hyper-V Server 2012 (Hyper-V Hypervisor)

VNMC can be installed on the VMWare Hypervisor and the Hyper-V Hypervisor. The following table lists some of the VNMC features that are not supported when VNMC is installed on the HyperV Hypervisor.

When doing the following...	This feature is unsupported
Adding a rule to the create the ACL policy	• The option to match any one rule is disabled. The only available option is to match all the rules. • The service condition is disabled. • When you are setting source or destination conditions, the VM and User Defined attribute types are not supported. • VM Manager actions are not supported.
Adding an object group	• When the attribute type is Network, the attribute name Service is not supported. • The VM attribute type is not supported.
Working with vZones	The option to match any one rule is disabled. The vZone must match all conditions.

Search

The Search tab enables you to search for instances of organizations in VNMC. From the search result, you can expand an organization's hierarchy and launch devices and polices in that organization.

Note Searching for organization names does not work if the organization names contain special characters.

Procedure

Step 1 Do any of the following to launch the Search tab:

- Choose **Policy Management > Service Policies > root > Search**.
- Choose **Policy Management > Service Profiles > root > Search**.
- Choose **Policy Management > Device Configurations > root > Search**.
- Choose **Tenant Management > root > Search**.
- Choose **Resource Management > Managed Resources > root > Search**.

Note You can perform the Search operation at any level in the organizational hierarchy.

Step 2 Enter organization names as a *pattern or a regular expression.
The Search feature is case-sensitive. When you enter a name as a regular expression, it can contain regex wildcards such as * , + , ? and so on. For example, "*" will match the previous character zero or more times. Searching myVdc* will return all names that contain "myVd" and "myVDC".

Use the following the guidelines when you enter a pattern:

- To fetch organization names starting with "ABC", enter "ABC*".
- To fetch organization names ending with "ABC", enter "*ABC".
- To fetch organizations names starting with "A" and ending with "BC" but with other characters in between, enter "A*BC".

Step 3 Click **Search**.
The search results are displayed in the table.

Clone

You can create a clone for an organization, policy, policy set, or profile at a destination of your choice. The hierarchy of an organization's clone or the names of the elements in it cannot be changed. After a clone is created, it cannot be renamed or moved to another location.

Procedure

Step 1 Based on the element you want to clone, do one of the following:

- To clone an organization, choose **Tenant Management > root > *tenant* > *organization***.
- To clone a policy, policy set, or profile, choose **Policy Management > Service Polices > root > *tenant* > Policies > *policy*** or **Policy Management > Service Profiles > root > *tenant* > Profiles > *profile***.

Step 2 Right-click the element to be cloned and choose **Clone**.

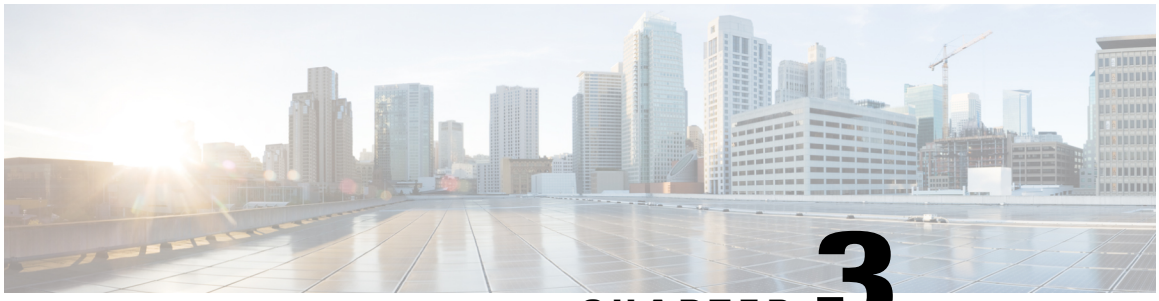
Step 3 In the Clone dialog box that appears:

a) Enter the name and destination of the clone.

b) Click **OK**.

The clone appears in the destination you chose.

Clone



CHAPTER 3

Configuring Primary Authentication

This section includes the following topics:

- Primary Authentication, page 13
- Remote Authentication Providers, page 13
- Creating an LDAP Provider, page 14
- Editing an LDAP Provider, page 16
- Deleting an LDAP Provider, page 17
- Selecting a Primary Authentication Service, page 17

Primary Authentication

VNMC supports two methods to authenticate user logins:

- Local to VNMC
- Remote through LDAP

The role and locale assignment for a local user can be changed on VNMC. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Remote Authentication Providers

If a system is configured for a supported remote authentication service, you must create a provider for that service to ensure that VNMC and the system configured with the service can communicate.

User Accounts in Remote Authentication Services

You can create user accounts in VNMC or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through the VNMC GUI.

User Roles and Locales in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles and locales those users require for working in VNMC and that the names of those roles and locales match the names used in VNMC. If an account does not have the required roles and locales, the user is granted only read-only privileges.

LDAP Attribute for User

In VNMC, the LDAP attribute that holds the LDAP user roles and locales is preset. This attribute is always a name-value pair. For example, by default CiscoAvPair specifies the role and locale information for the user, and if the filter is specified, the LDAP search is restricted to those values that match the defined filter. By default, the filter is sAMAccountName=$userid. The user can change these values to match the setting on the LDAP server. When a user logs in, VNMC checks for the value of the attribute when it queries the remote authentication service and validates the user. The value should be identical to the username.

An example of LDAP property settings is as follows:

- Timeout—30
- Retries—1
- Attribute—CiscoAvPair
- Filter—sAMAccountName=$userid
- Base DN—DC=cisco, DC=com (The specific location in the LDAP hierarchy where VNMC starts the query for the LDAP user.)

Creating an LDAP Provider

Before You Begin

Configure users with the attribute that holds the user role and locale information for VNMC. You can use an existing LDAP attribute that is mapped to the VNMC user roles and locales, or you can create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1. When you add the LDAP user to the LDAP server, specify the role and locale in the attribute (for example, shell:roles=network,aaa shell:locale=sanjose,dallas).

Procedure

Step 1 Choose **Administration > Access Control > LDAP**.

Step 2 In the content pane, click **Create LDAP Provider**.

Step 3 In the Create LDAP Provider dialog box, provide the following information:

Field	Description
Hostname/IP Address	Hostname or IP address of the LDAP provider. If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname instead of an IP address, you must configure a DNS server in the VNMC server.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.
Root DN	Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 127 characters.
Port	Port through which VNMC communicates with the LDAP database. The default port number is 389.
Enable SSL	Check to enable SSL.

Note Depending on the object you select in the table, different options appear above the table.

Step 4 Click **OK**, then click **Save**.

Following is an example of creating an LDAP provider:

- **Hostname/IP Address—**Provider-blr-sam-aaa-10.cisco.com
- **Key—**xxxxxx (The password of the LDAP database account specified in the **Root DN** field.)
- **Root DN—** CN=bob,DC=cisco,DC=com (The value of CN is the name of a user with query privileges. DC refers to the location in the LDAP directory where a user is created.)
- **Port—**389
- **Enable SSL—**check box

What to Do Next

Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, on page 17.

Editing an LDAP Provider

Procedure

Step 1 Choose **Administration > Access Control > LDAP**.

Step 2 In the content pane, select the required LDAP provider.

Step 3 Click **Edit**.

Step 4 In the Edit dialog box, modify the settings as required, using the following table as a guide:

Field	Description
Name	Hostname or IP address of the LDAP provider (read-only). If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname instead of an IP address, you must configure a DNS server in the VNMC server.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.
Set	Whether or not the preshared key has been set and is properly configured (read-only). If the Set value is Yes, and the Key field is empty, it indicates that a key was provided previously.
Root DN	Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 127 characters.
Port	Port through which VNMC communicates with the LDAP database. The default port number is 389.
Enable SSL	Check to enable SSL.

Step 5 Click **OK**, then click **Save.**

Deleting an LDAP Provider

Procedure

Step 1 In the Administration tab, choose **Access Control > LDAP**.

Step 2 In the Work pane, select the LDAP provider that you want to delete, then click **Delete**.

Step 3 Confirm the deletion, then click **Save**.

Selecting a Primary Authentication Service

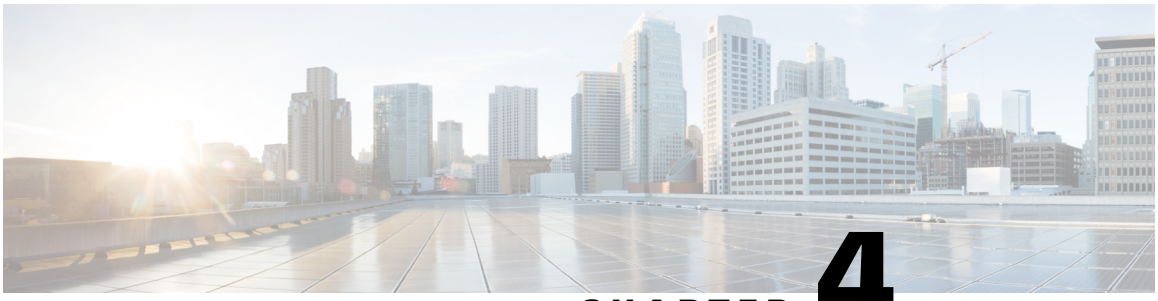
Note If the default authentication is set to LDAP, and the LDAP servers are not operating or are unreachable, the local admin user can log in at any time and make changes to the authentication, authorization, and accounting (AAA) system.

Procedure

Step 1 Choose **Administration > Access Control > Authentication**.

Step 2 In the Properties tab, specify the information as described in the following table, then click **OK**.

Field	Description
Default Authentication	Default method by which a user is authenticated during remote login: • LDAP—The user must be defined on the LDAP server specified for this VNMC instance. • Local—The user must be defined locally in this VNMC instance. • None—A password is not required when the user logs in remotely.
Role Policy to Remote Users	Action taken when a user attempts to log in and the LDAP server does not supply a user role with the authentication information: • assign-default-role—The user is allowed to log in with a read-only user role. • no-login—The user is not allowed to log into the system, even if the user name and password are correct.



CHAPTER 4

Configuring RBAC

This section contains the following topics:

- RBAC, page 19
- User Accounts, page 19
- User Roles, page 21
- Privileges, page 22
- User Locales, page 23
- Configuring User Roles, page 24
- Configuring User Locales, page 26
- Configuring Locally Authenticated User Accounts, page 28
- Monitoring User Sessions, page 32

RBAC

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts

User accounts are used to access the system. Up to 128 local user accounts can be configured in each VNMC instance. Each user account must have a unique username.

A local user can be authenticated using a password or an SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Default User Account

Each VNMC instance has a default user account, admin, which cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

Username Guidelines

The username is also used as the login ID for VNMC. When you assign usernames to VNMC user accounts, consider the following guidelines and restrictions:

- The login ID can contain from 1 to 32 characters, including the following:
  - Any alphanumeric character
  - Period (.)
  - Underscore (_)
  - Dash (-)
  - At symbol (@)
- Neither the unique username nor a local user's username can consist solely of numbers.
- The unique username cannot start with a number.
- If an all-numeric username exists on a AAA server (LDAP) and is entered during login, VNMC cannot log in the user.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

Note You can create up to 128 user accounts in a VNMC instance.

Password Guidelines

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password must be strong. If the Password Strength Check option is enabled, VNMC rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters.

- Must contain at least three of the following:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: dollar sign ($), question mark (?), or equals sign (=).
- Should not be blank for local user and admin accounts.

Note The Password Strength Check option is enabled by default. You can disable it from the Locally Authenticated Users pane (Administration > Access Control > Locally Authenticated Users).

Note If VNMC is configured to use remote authentication with LDAP, passwords for those remote accounts can be blank. With this configuration, the remote credentials store is used for authentication only, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy- and tenant-related privileges.

All roles include read access to all configuration settings in the VNMC instance. The difference between the read-only role and other roles is that a user who is assigned only the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

The system contains the following default user roles:

aaa

Users have read and write access to users, roles, and AAA configuration, and read access to the rest of the system.

admin

Users have read and write access to the entire system and has most privileges. However, users cannot create or delete files, or perform system upgrades. These functions can be done only through the default admin account. The default admin account is assigned this role by default, and it cannot be changed.

network

Users can create organizations, security policies, and device profiles.

operations

Users can acknowledge faults and perform some basic operations, such as logging configuration.

read-only

Users have read-only access to system configuration and operational status with no privileges to perform any operations.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

The role and locale assignment for a local user can be changed on VNMC. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Privileges

User Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and its description.

Privilege Name	Description
AAA	System security and AAA.
Admin	System administration.
read-only	Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role.
Resource Configuration	Edge and compute firewall configuration.
Policy Management	Edge and compute firewall policies.

Privilege Name	Description
Fault Management	Alarms and alarm policies.
Operations	Logs, core file management, and **show tech-support** command.
Tenant Management	Create, delete, and modify tenants and organization containers.

Privileges and Role Assignments

The following table lists the out-of-box default role name for each privilege.

Default Role Name	Privilege Name
aaa	aaa
admin	admin
network	policy, res-config, tenant
operations	fault, operations
read-only	read-only

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations or domains (collectively referred to as *resources*) to which the user is allowed access. In addition, the user has read-only access privileges outside their assigned locale and going up the organization tree. This enables the user to use these resources when creating policies. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations. Only the objects under organizations are controlled by locales. Access to other objects such as users, roles, and resources that are not present in the organization tree are not affected by locales.

Note Users not assigned to a locale have access to all resources in all organizations. For users assigned to a locale, access is restricted to the objects that reside under the organizations that belong to that locale.

Users with AAA privileges (AAA role) can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization, then a user assigned that locale can assign only the Engineering organization to other users.

Note AAA privileges must be carefully assigned because they allow a user to manage other users' privileges and role assignments.

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

The role and locale assignment for a local user can be changed on VNMC. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Configuring User Roles

Creating a User Role

Procedure

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Click **Create Role**.

Step 3 In the Create Role dialog box, complete the following fields, then click **OK**:

Field	Description
Name	User role name.

Field	Description
Privileges	Available privileges. To assign a privilege to the selected role, check one or more of the following check boxes: • Admin • AAA • Fault Management • Operations • Policy Management • Resource Configuration • Tenant Management **Note** You can assign the admin privilege, which includes all privileges, or you can assign privileges individually.

Editing a User Role

Procedure

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Select the role you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, check or uncheck the boxes for the privileges you want to add to or remove from the role, then click **OK**.

Deleting a User Role

Except for the admin and read-only roles, you can delete user roles that are not appropriate for your environment.

Procedure

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Select the user role you want to delete, then click **Delete**.

Note You cannot delete the admin or read-only role.

Step 3 In the Confirm dialog box, click **Yes**.

Configuring User Locales

Creating a Locale

Before You Begin

Verify that one or more organizations (tenants) exist; if none exist, create one. For information on creating tenants, see Creating a Tenant, on page 70.

Procedure

Step 1 Choose **Administration > Access Control > Locales**.

Step 2 Click **Create Locale**.

Step 3 In the Create Locale dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Locale name, containing 2 to 255 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change this name after it is saved.
Description	Brief locale description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Assigned Organizations	
Assign Organization	Click to assign organizations to locales.
Assigned Organization	List of organizations assigned to the locale.

What to Do Next

Add the locale to one or more user accounts. For more information, see Changing the Locales or Roles Assigned to a Locally Authenticated User, on page 32.

Editing a Locale

Procedure

Step 1 Choose **Administration > Access Control > Locales**.

Step 2 In the list of locales, select the locale you want to edit, then click **Edit**.

Step 3 In the Description field, change the description as appropriate.

Step 4 Click **Assign Organization**.

Step 5 In the Assign Organization dialog box:

a) Expand the root node to view the available organizations.

b) Check the check boxes of the organizations to assign to the locale.

Step 6 Click **OK** in the open dialog boxes to save your changes.

Deleting a Locale

Before You Begin

Caution If the locale you want to delete is assigned to any user/s, remove the locale from the user list of locales.

Procedure

Step 1 In the Navigation pane, click the **Administration** tab.

Step 2 In the Navigation pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, click the **Locales** node.

Step 4 In the **Work** pane, click the locale you want to delete.

Step 5 Click **Delete.**

Step 6 In the **Confirm** dialog box, click **Yes**.

Assigning an Organization to a Locale

Procedure

Step 1 Choose **Administration > Access Control > Locales >** *locale*.

Step 2 Click **Assign Organization**.

Step 3 In the Assign Organization dialog box:

a) Expand root to view the available organizations.

b) Check the check boxes for the organizations you want to add to the locale.

Step 4 Click **OK** in the open dialog boxes, then click **Save** to save the locale.

Deleting an Organization from a Locale

Procedure

Step 1 Choose **Administration > Access Control > Locales >** *locale*.

Step 2 In the content pane, click the **General** tab.

Step 3 In the Assigned Organizations area, select the organization you want to delete, then click **Delete Organization**.

Step 4 When prompted, confirm the deletion.

Step 5 Click **Save**.

Configuring Locally Authenticated User Accounts

Creating a User Account

Procedure

Step 1 Choose **Administration > Access Control > Locally Authenticated Users**.

Step 2 Click **Create Locally Authenticated Users**.

Step 3 In the Properties area, complete the following fields:

Field	Description
Login ID	Login name. This name must be unique and meet the following guidelines and restrictions for VNMC user accounts: • The login ID can be between 1 and 32 characters, including the following: ◦ Any alphanumeric character ◦ Underscore (_) ◦ Dash (-) ◦ At symbol (@) • The user name for each user account cannot be all-numeric. • The user name cannot start with a number. After you save the user name, it cannot be changed. You must delete the user account and create a new one.
Description	User description.
First Name	User first name. This field can contain up to 32 characters.
Last Name	User last name. This field can contain up to 32 characters.
Email	User email address.
Phone	User telephone number.

Field	Description
Password	Password associated with this account. For maximum security, each password must be strong. If the Password Strength Check check box is checked, the system rejects any password that does not meet the following requirements: • Contains a minimum of eight characters • Contains at least three of the following: ◦ Lowercase letters ◦ Uppercase letters ◦ Digits ◦ Special characters • Does not contain a character that is repeated more than three times consecutively, such as aaabbb. • Is not the user name or the reverse of the user name. • Passes a password dictionary check. For example, the password must not be based on a standard dictionary word. • Does not contain the following symbols: dollar sign ($), question mark (?), equals sign (=). • The password must not be blank for local user and admin accounts. **Note** The password strength check box on the Locally Authenticated Users pane can be unchecked, indicating that the password is not required to be strong. It must, however, contain a minimum of eight characters. The password field is a required field, and a user cannot be created without providing a password.
Confirm Password	Reenter the password for confirmation purposes.
Password Expires	Indicates whether or not password expiration is enabled. Check the check box to enable password expiration.
Expiration Date	Available if password expiration is enabled. Date that the password expires.

Step 4 In the **Roles/Locales** tab area, complete the following fields:

Field	Description
Assigned Roles	Check the applicable check boxes to assign one or more roles to the user: • aaa • admin • network • operations • read-only
Assigned Locale	Check the applicable check boxes to assign one or more locales to the user.

Step 5 In the **SSH** tab area, complete the following fields:

Field	Description
Key	SSH key. If you choose the Key radio button, the SSH Data field is displayed.
Password	SSH password.
SSH Data	Available if Key is selected. Enter the SSH public key.

Step 6 Click **OK**.

Changing the Locales or Roles Assigned to a Locally Authenticated User

Procedure

Step 1 Choose **Administration > Access Control > Locally Authenticated Users >** *user*.
Step 2 In the General tab, click the **Roles/Locales** tab.
Step 3 Check or uncheck the appropriate check boxes to assign or remove a locale or role.
Step 4 Click **Save**.

Changing the Roles Assigned to a Locally Authenticated User Account

Procedure

Step 1 In the Navigation pane, click the **Administration** tab.
Step 2 In the Navigation pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, expand the **Locally Authenticated Users** node.
Step 4 Click the *User_name* you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Click the **Roles/Locales** tab.
Step 7 In the **Assigned Role(s)** area, do the following:

- To assign a new role to the user account, check the appropriate check boxes.
- To remove a role from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Monitoring User Sessions

You can monitor sessions for both locally and remotely authenticated users.

Procedure

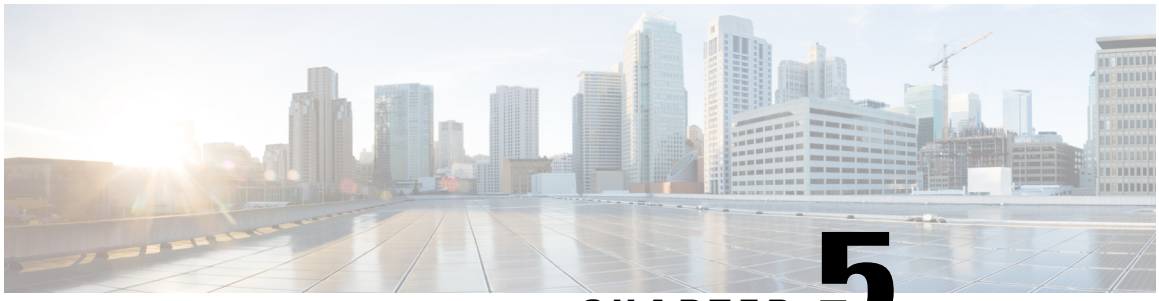
Step 1 Choose **Administration > Access Control**, then choose one of the following:

- **Locally Authenticated Users >** *user*.

- **Remotely Authenticated Users >** *user*.

Step 2 Click the **Sessions** tab to view the user session.

Field	Description
Host	IP address from which the user is logged in.
Login Time	Date and time the session started.
UI	User interface for this session: • web—GUI login • shell—CLI login • ep—End point
Terminal Type	Kind of terminal through which the user is logged in.



CHAPTER 5

Configuring Trusted Points

This section includes the following topics:

- Trusted Points, page 35
- Configuring Trusted Points, page 35

Trusted Points

When setting up LDAP over Secure Sockets Layer (SSL) protocol for VNMC user authentication, you need to create a trusted point for each LDAP server. The certificate in the trusted point can be any one of the following:

- The certificate of the certificate authority (CA) that issued the LDAP server certificate.
- If the CAs are organized in a hierarchy, the certificate of any of the CAs in the hierarchy.
- The certificate of the LDAP server.

Configuring Trusted Points

Creating a Trusted Point

Procedure

Step 1 Choose **Administration > Access Control > Trusted Point**.

Step 2 Click **Create Trusted Point**.

Step 3 In the Create Trusted Point dialog box, complete the following fields, then click **OK**.

Field	Description
Name	Trusted point name.

Field	Description
Certificate Chain	Certificate information for this trusted point.

Editing a Trusted Point

Procedure

Step 1 Choose **Administration > Access Control > Trusted Point**.

Step 2 In the content pane, choose the required trusted point, then click **Edit**.

Step 3 In the Edit dialog box, modify the certificate chain as appropriate, then click **OK**.
The Name and Fingerprint fields cannot be modified.

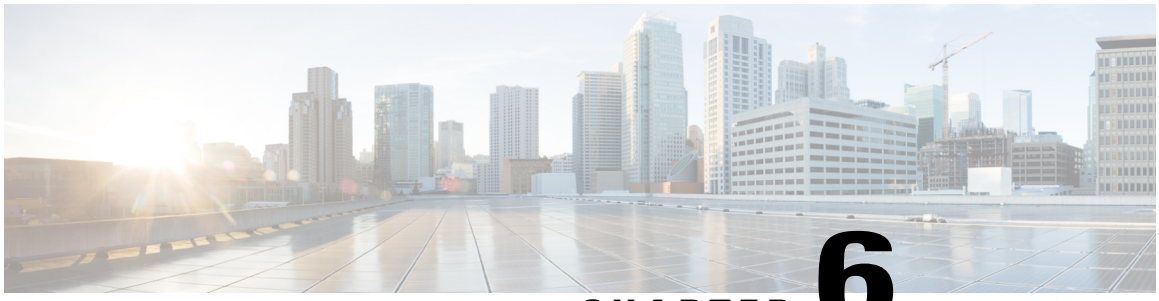
Deleting a Trusted Point

Procedure

Step 1 Choose **Administration > Access Control > Trusted Point**.

Step 2 In the content pane, select the trusted point you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.



CHAPTER 6

Configuring VNMC Profiles

This section includes the following topics:

- Profiles, page 37
- Policies in VNMC Profiles, page 37
- Configuring Policies, page 38
- Configuring the Default Profile, page 56

Profiles

VNMC profiles are configurable.

VNMC provides default profiles. Default profiles are system generated and can be modified, but they cannot be deleted. You can add new policies to a profile, including DNS and NTP policies, or assign existing policies to the a profile.

The VNMC profile includes the DNS domain name that specified at boot configuration. That domain is displayed in the VNMC instance. New DNS domains cannot be created. However, the domain name description can be modified.

VNMC does not support the creation of additional VNMC profiles.

Policies in VNMC Profiles

You can create multiple policies and assign them to the VNMC profile. Policies for the VNMC profile are created and deleted on the **VNMC Profile** tab. Policies can be assigned to the VNMC profile. VNMC profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-Tenant Environment, on page 70.

The following policies created under root only, in the Device Policies area, will be visible in the VNMC profile:

- Core file policy
- Fault policy

- Logging policy
- Syslog policy

Policies created under root are visible to both the VNMC profile and the Device profile.

DNS server, NTP server and domain names can be assigned as inline policies. A time zone setting can also be assigned to the profile.

When the system boots up, the following policies already have existing default policies:

- Fault policy
- Logging policy
- Syslog policy

The default policies cannot be deleted but may be modified.

Configuring Policies

Configuring a Core File Policy

Adding a Core File Policy to the VNMC Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Core File**.

Step 2 In the General tab, click **Add Core File Policy**.

Step 3 In the Add Core File Policy dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved.
Description	Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.).
Admin State	Indicate whether the administrative state of the policy is to be enabled or disabled.
Hostname	Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in VNMC.

Field	Description
Port	Port number for sending the core dump file.
Protocol	Protocol for exporting the core dump file (read-only).
Path	Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/*test*, where *test* is the subfolder.

Editing a Core File Policy for a VNMC Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Core File**.

Step 2 In the General tab, click the core file policy you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, modify the following fields as appropriate, then click **OK**:

Field	Description
Name	Name of the core file policy (read-only).
Description	Brief policy description.
Admin State	Administrative status of the policy: enabled or disabled.
Hostname	Hostname or IP address. **Note** If you use a hostname, you must configure a DNS server.
Port	Port number to use when exporting the core dump file.
Protocol	Protocol used to export the core dump file (read-only).
Path	Path to use when storing the core dump file on the remote system. The default path is /tftpboot. To specify a subfolder under tftpboot, use the format /tftpboot/*folder* where *folder* is the subfolder.

Deleting a Core File Policy from the VNMC Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Core File**.

Step 2 In the General tab, click the core file policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring a Fault Policy

Adding a Fault Policy to the VNMC Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Fault**.

Step 2 In the General tab, click **Add Fault Policy**.

Step 3 In the Add Fault Policy dialog box, provide the information as described in the following table, then click **OK**:

Field	Description
Name	Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief policy description.

Field	Description
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Action to be taken when faults are cleared: • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared.
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Editing a Fault Policy for a VNMC Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Fault**.

Step 2 In the General tab, select the fault policy you want to edit, then click **Edit**.

Step 3 In the Edit Fault Policy dialog box, modify the fields as needed by using the information in the following table, then click **OK**.

Field	Description
Name	Policy name (read-only).
Description	Brief policy description.
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition recurs during the flapping interval, the fault returns to the active state. If the condition does not recur during the flapping interval, the fault is cleared. The next action depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Available fault retention actions: • retain—The system retains fault messages. • delete—The system deletes fault messages when they are marked as cleared.
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Deleting a Fault Policy from the VNMC Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Fault**.

Step 2 In the General tab, select the fault policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring a Logging Policy

Adding a Logging Policy to the VNMC Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Log File**.

Step 2 In the General tab, click **Add Logging Policy**.

Step 3 In the Add Logging Policy dialog box, complete the following fields:

Field	Description
Name	Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief policy description.

Field	Description
Log Level	One of the following logging severity levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Step 4 Click **OK**.

Editing a Logging Policy for VNMC Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Log File**.

Step 2 In General tab, select the logging policy that you want to edit, then click **Edit**.

Step 3 In the Edit Log File Policy dialog box, modify the information as required by using the information in the following table, then click **OK**.

Field	Description
Name	Logging policy name (read-only).
Description	Brief policy description.
Log Level	One of the following logging levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Deleting a Logging Policy from the VNMC Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Log File**.

Step 2 In the General tab, select the logging policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring a Syslog Policy

Adding a Syslog Policy to the VNMC Profile

The syslog message settings that you configure for the VNMC profile apply to VNMC syslog messages only. These settings do not affect other non-VNMC syslog messages.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Syslog**.

Step 2 In the General tab, click **Add Syslog Policy**.

Step 3 In the Add Syslog Policy dialog box, provide the information as described in the following table, then click **OK**.

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.

Field	Description
Local Destinations Tab	
Console area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
Monitor area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
File area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.

Editing a Syslog Policy for the VNMC Profile

The syslog message settings that you configure for the VNMC profile apply to VNMC syslog messages only. These settings do not affect other non-VNMC syslog messages.

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Syslog**.

Step 2 In the General tab, select the syslog policy you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, update the information as required by using the information in the following table, then click **OK**.

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.

Field	Description
Monitor area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
File area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.

Deleting a Syslog Policy from a VNMC Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Syslog**.

Step 2 In the General tab, click the syslog policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding a Syslog Server to the VNMC Profile

This procedure assumes that you have already created a syslog policy for a VNMC profile. For information on creating a syslog policy for a VNMC profile, see Adding a Syslog Policy to the VNMC Profile, on page 46.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Syslog >** *syslog-policy*.

Step 2 In the Servers tab, click **Add Syslog Server**.

Step 3 In the Add Syslog Server dialog box, provide the information as described in the following table, then click **OK**:

Field	Description
Server Type	One of the following server types: • primary • secondary • tertiary
Hostname/IP Address	Hostname or IP address where the syslog file resides. **Note** If you use a hostname, you must configure a DNS server.
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)

Field	Description
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	Administrative state of the server: enabled or disabled.
Port	Port to use to send data to the syslog server. The default port selection is 514 for UDP.
Protocol	Protocol to use: TCP or UDP (default).
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.
Server Interface	Interface to use to access the syslog server.

Editing a Syslog Server for the VNMC Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Syslog**.

Step 2 In the General tab, select the syslog policy with the syslog server that you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.

Step 4 Select the syslog server that you want to edit, then click **Edit**.

Step 5 In the Edit Syslog Server dialog box, edit the information as required, using the information in the following table, and then click **OK**:

Field	Description
Server Type	One of the following server types: primary, secondary, or tertiary.
Hostname/IP Address	Hostname or IP address where the syslog file resides. **Note** If you use a hostname, you must configure a DNS server.
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)

Field	Description
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	Administrative state of the server: enabled or disabled.
Port	Port to use to send data to the syslog server. The default port selection is 514 for UDP.
Protocol	Protocol to use: TCP or UDP (default).
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.

Field	Description
Server Interface	Interface to use to access the syslog server. This option applies to ASA 1000V only. Enter the data interface name specify in the edge firewall. Use the device CLI to configure a route through the management interface.

Deleting a Syslog Server from a VNMC Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Policies > Syslog**.
Step 2 In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.
Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.
Step 4 In the Servers table, select the syslog server you want to delete, then click **Delete**.
Step 5 When prompted, confirm the deletion.
Step 6 Click **OK** or **Apply** to apply the change to the syslog policy.

Configuring the Default Profile

Editing the VNMC Default Profile

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Profile > default**.
Step 2 In the General tab, update the information as required:

Field	Description
Name	Default profile name (read-only).
Description	Brief profile description.

Field	Description
Time Zone	Available time zones. The default time zone is UTC.

Step 3 In the Policy tab, update the information as required:

Field	Description
DNS Servers	
Add DNS Server	Click to add a new DNS server.
Delete	Deletes the DNS server selected in the DNS Servers table.
Up and down arrows	Changes the priority of the selected DNS server. VNMC uses the DNS servers in the order in which they appear in the table.
DNS Servers table	Identifies the DNS servers configured in the system.
NTP Servers	
Add NTP Server	Click to add a new NTP server.
Delete	Deletes the NTP server selected in the NTP Servers table.
Up and down arrows	Changes the priority of the selected NTP server. VNMC uses the NTP servers in the order in which they appear in the table.
NTP Servers table	Identifies the NTP servers configured in the system.
DNS Domains	

Field	Description
Edit	Edits the DNS domain selected in the DNS Domains table. The default DNS domain cannot be deleted. **Caution** Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new VNMC certificate. This situation occurs when the VNMC hostname, VNMC domain name, or both have changed. The VM Manager Extension file must be exported again and installed on vCenter. To continue, accept the VNMC certificate and log into VNMC again.
DNS Domains	Identifies the default DNS domain name and domain configured in the system.
Other Options	
Syslog	The syslog policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Fault	The fault policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Core File	The core file policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Log File	The log file policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.

Step 4 Click **Save**.

Configuring a DNS Server

Adding a DNS Server

You an specify a maximum of four DNS servers for the VNMC profile. Use the up and down arrows to arrange the servers from highest to lowest priority, with the highest priority server at the top of the list.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Profile > default**.
Step 2 Click the **Policy** tab.
Step 3 In the DNS Servers area, click **Add DNS Server**.
Step 4 In the Add DNS Server dialog box, enter the DNS server IP address, then click **OK**.
Step 5 Click **Save**.

Deleting a DNS Server

Procedure

Step 1 Choose **Administration > VNMC Profile> root > VNMC Profile > default**.
Step 2 Click the **Policy** tab.
Step 3 In the **DNS Servers** area, select the DNS server you want to delete, then click **Delete**.
Step 4 When prompted, confirm the deletion.
Step 5 Click **Save** to save your changes.

Configuring an NTP Server

Adding an NTP Server

You can specify a maximum of four NTP servers for the VNMC profile. Use the up and down arrows to arrange the servers from highest to lowest priority, with the highest priority server at the top of the list.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Profile > default**.
Step 2 In the Policy tab, click **Add NTP Server**.
Step 3 In the Add NTP server dialog box, enter the hostname or IP address of the NTP server, then click **OK**.
Step 4 Click **Save**.

Deleting an NTP Server

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Profile > default**.
Step 2 Click the **Policy** tab.
Step 3 In the NTP Servers area, click the server that you want to delete, then click **Delete**.
Step 4 When prompted, confirm the deletion.
Step 5 Click **Save**.

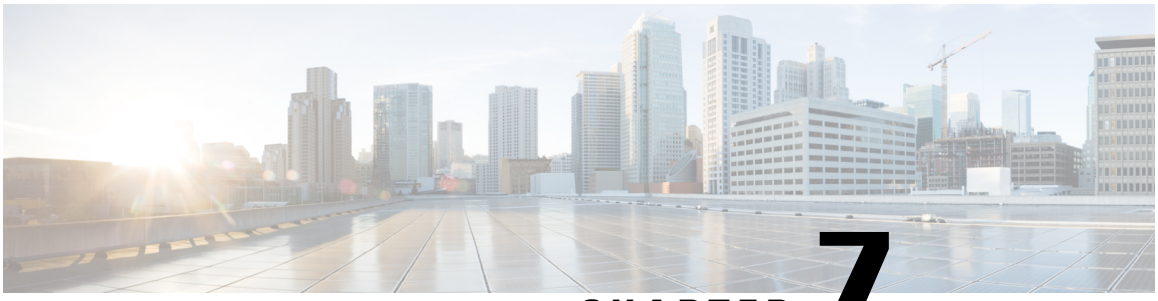
Configuring a DNS Domain

Editing a DNS Domain

Caution Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new VNMC certificate. This situation occurs when the VNMC hostname. VNMC domain name, or both have changed. The VM Manager Extension file must be exported again and installed on vCenter. To continue, accept the VNMC certificate and log into VNMC again.

Procedure

Step 1 Choose **Administration > VNMC Profile > root > VNMC Profile > default**.
Step 2 Click the **Policy** tab.
Step 3 In the DNS Domains table, select the domain that you want to edit, then click **Edit**.
Step 4 In the Edit DNS Domains dialog box, edit the Domain Name field as required, then click **OK**.
Step 5 Click **Save**.



CHAPTER 7

Configuring VM Managers

This section includes the following topics:

- VM Manager Overview, page 61
- Configuring VM Managers Under Administration, page 62
- Configuring VM Managers Under Resource Management, page 64

VM Manager Overview

Note This feature is not supported on Hyper-V Hypervisor.

VNMC connects to vCenter on port 80. A vCenter extension file is required to establish a connection between VNMC and vCenter. The extension file is exported from VNMC and linked on the VM Managers tab. You install the vCenter extension file as a plugin on all vCenter servers to which you want to connect.

You can configure a VM Manager (vCenter) in VNMC under Administration or Resource Management, depending on your environment and requirements. For more information, see the following topics:

- Adding a VM Manager Under Administration, on page 62
- Adding a VM Manager Under Resource Management, on page 64

Note In VMware, a VM can be nested within resources. However, when you view the VM properties in VNMC, only the higher level resource is displayed. For example, you can add a VM that is part of a resource pool that resides in a virtual application (vApp). When you view this VM in VNMC, only the vApp name is displayed and not that of the resource pool.

Configuring VM Managers Under Administration

Adding a VM Manager Under Administration

This procedure describes how to add a VM Manager under Administration. For information on adding a VM Manager under Resource Management, see Adding a VM Manager Under Resource Management, on page 64.

Before You Begin

A vCenter extension file is required to establish a secure connection between the vCenter and the VM Manager. Export the vCenter extension file by clicking **Export vCenter Extension**, and installing it as a plugin on all the vCenter servers.

You can find the Export vCenter Extension option in the following locations:

- Choose **Resource Management > Resources > Virtual Machines > VM Managers**.
- Choose **Administration > VM Managers > VM Managers**.

For detailed information on configuring VNMC connectivity with vCenter, see the *Cisco Virtual Network Management Center Quick Start Guide*, available at http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html.

Procedure

Step 1 Choose **Administration > VM Managers > VM Managers**.

Step 2 Click **Add VM Manager**.

Step 3 In the Add VM Manager dialog box, complete the following fields, then click **OK**:

Field	Description
Name	VM Manager name, containing 2 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	VM Manager description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Hostname/IP Address	Hostname or IP address of the VM Manager.
Port Number	Port to use for communications with the VM Manager.

After you add a VM Manager, VNMC fetches the VMs available on vCenter with Nexus 1000V port profiles attached, and displays them under Resource Management > Resources > Virtual Machines.

Editing a VM Manager

When you edit a VM Manager, you can change its administrative state as long as the VM Manager has the appropriate operational state:

- To change the administrative state to enabled, the operational state must be down.
- To change the administrative state to disabled, the operational state must be up.

If your request to change the administrative state fails, resubmit the request when the system has the correct operational state.

Procedure

Step 1 Choose **Administration > VM Managers > VM Managers**.

Step 2 In the VM Managers tab, select the VM Manager you want to edit, then click **Edit**.

Step 3 In the Edit VM Manager dialog box, edit the information as required, then click **OK**.

Field	Description
Name	VM Manager name (read-only).
Description	Description of the VM Manager.
Hostname/IP Address	VM Manager hostname or IP address (read-only).
Port Number	Port to use for communications with the VM Manager (read-only).
Admin State	One of the following administrative states for the VM Manager: • enable—When a vCenter is added to VNMC with the administrative state of enable, the system fetches all VM inventory from vCenter. Any changes that occur to the VM on vCenter are also fetched. • disable—When a vCenter is added to VNMC with the administrative state of disable, the system displays all discovered VMs from vCenter. Any changes that occur to the VMs on the vCenter are not fetched. The changes will be fetched by VNMC when the admin state is changed to enable.

Field	Description
Type	VM Manager vendor (read-only).
Version	VM Manager version (read-only).
Operational State	One of the following operational states (read-only): • up • unreachable • bad-credentials • comm-err • admin-down • unknown
Operational State Reason	Provides the reason for the operational state if the operational state is anything other than *up* (read-only).

Deleting a VM Manager

Procedure

Step 1 Choose **Administration > VM Managers > VM Managers**.

Step 2 In the VM Managers tab, select the VM Manager you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring VM Managers Under Resource Management

Adding a VM Manager Under Resource Management

This procedure describes how to add a VM Manager under Resource Management. For information on installing a VM Manager under Administration, see Adding a VM Manager Under Administration, on page 62.

Before You Begin

A vCenter extension file is required to establish a secure connection between the vCenter and the VM Manager. Export the vCenter extension file by clicking **Export vCenter Extension**, and installing it as a plugin on all the vCenter servers.

You can find the Export vCenter Extension option in the following locations:

- Choose **Resource Management > Resources > Virtual Machines > VM Managers**.
- Choose **Administration > VM Managers > VM Managers**.

For detailed information on configuring VNMC connectivity with vCenter, see the *Cisco Virtual Network Management Center Quick Start Guide*, available at http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html.

Procedure

Step 1 Choose **Resource Management > Resources > Virtual Machines > VM Managers**.

Step 2 Click **Add VM Manager**.

Step 3 In the Add VM Manager dialog box, complete the following fields, then click **OK**:

Field	Description
Name	VM Manager name, containing 2 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	VM Manager description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Hostname/IP Address	Hostname or IP address of the VM Manager.
Port Number	Port to use for communications with the VM Manager.

After you add a VM Manager, VNMC fetches the VMs available on vCenter with Nexus 1000V port profiles attached, and displays them under Resource Management > Resources > Virtual Machines.

Editing a VM Manager

When editing a VM Manager, you can change its administrative state as long as it has the appropriate operational state:

- To change the administrative state to enabled, the operational state must be down.

- To change the administrative state to disabled, the operational state must be up.

If your request to change the administrative state fails, resubmit the request when the system has the correct operational state.

Procedure

Step 1 Choose **Resource Management > Resources > Virtual Machines > VM Managers**.

Step 2 In the VM Managers tab, select the VM Manager you want to edit, then click **Edit**.

Step 3 In the Edit VM Manager dialog box, edit the information as required, then click **OK**.

Field	Description
Name	VM Manager name (read-only).
Description	Description of the VM Manager.
Hostname/IP Address	VM Manager hostname or IP address (read-only).
Port Number	Port to use for communications with the VM Manager (read-only).
Admin State	One of the following administrative states for the VM Manager: • enable—When a vCenter is added to VNMC with the administrative state of enable, the system fetches all VM inventory from vCenter. Any changes that occur to the VM on vCenter are also fetched. • disable—When a vCenter is added to VNMC with the administrative state of disable, the system displays all discovered VMs from vCenter. Any changes that occur to the VMs on the vCenter are not fetched. The changes will be fetched by VNMC when the admin state is changed to enable.
Type	VM Manager vendor (read-only).
Version	VM Manager version (read-only).

Field	Description
Operational State	One of the following operational states (read-only): • up • unreachable • bad-credentials • comm-err • admin-down • unknown
Operational State Reason	Provides the reason for the operational state if the operational state is anything other than *up* (read-only).

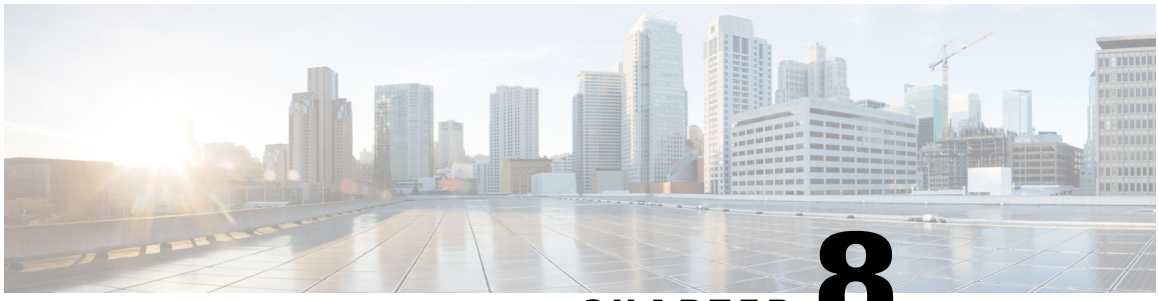
Deleting a VM Manager

Procedure

Step 1 Choose **Resource Management > Resources > Virtual Machines > VM Managers**.

Step 2 In the VM Managers tab, select the VM Manager you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.



CHAPTER 8

Configuring Tenants

This section includes the following topics:

- Tenant Management, page 69
- Configuring Tenants, page 70
- Configuring Virtual Data Centers, page 72
- Configuring Applications, page 73
- Configuring Tiers, page 74

Tenant Management

Tenant Management and Multi-Tenant Environments

VNMC provides the ability to support multi-tenant environments. A multi-tenant environment enables the division of large physical infrastructures into logical entities called organizations. As a result, you can achieve logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

The administrator can assign unique resources to each tenant through the related organization in the multi-tenant environment. These resources can include different policies, pools, device profiles, firewalls, and so on. The administrator can use locales to assign or restrict user privileges and roles by organization if access to certain organizations needs to be restricted.

VNMC provides a strict organizational hierarchy as follows:

1. Root
2. Tenant
3. Virtual Data Center
4. Application
5. Tier

The root can have multiple tenants. Each tenant can have multiple data centers. Each data center can have multiple applications, and each application can have multiple tiers.

The policies and pools created at the root level are systemwide and are available to all organizations in the system. However, any policies and pools created in an organization below the root level are available only to those resources that are below that organization in the same hierarchy.

For example, if a system has tenants named Company A and Company B, Company A cannot use any policies created in the Company B organization. Company B cannot access any policies created in the Company A organization. However, both Company A and Company B can use policies and pools in the root organization.

Name Resolution in a Multi-Tenant Environment

In a multi-tenant environment, VNMC uses the hierarchy of an organization to resolve the names of policies and resource pools. The steps VNMC takes to resolve the names of policies and resource pools are as follows:

1. VNMC checks the policies and pools for the specified name within an organization assigned to the device profile or security policy.
2. If the policy or pool is found, VNMC uses that policy or pool.
3. If the policy or pool does not contain available resources at the local level, VNMC moves up the hierarchy to the parent organization and checks for a policy with the specified name. VNMC repeats this step until the search reaches the root organization.

Note The object name reference resolution takes an object name and resolves an object from an organization container to the object with the same name which is closest in the tree up to the root of the tree. If an object with the specified name is not found, VNMC uses a corresponding default object. For example, there is an SNMP policy under data center called MySNMP, and there is an SNMP policy in the tenant in the same tree that is also MySNMP. In this case, the user cannot explicitly select the MySNMP policy under the tenant. If the user wants to select the SNMP policy under the tenant, they must provide a unique name for the object in the given tree.

4. If the search reaches the root organization and an assigned policy or pool is not found, VNMC looks for a default policy or pool starting at the current level and going up the chain to the root level. If a default policy or pool is found, VNMC uses it. If a policy is not available, a fault is generated.

Configuring Tenants

Creating a Tenant

Procedure

Step 1 Choose **Tenant Management > root > Create Tenant**.

Step 2 In the Create Tenant dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Tenant name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief tenant description. This field can contain between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon.

Editing a Tenant

Procedure

Step 1 Choose **Tenant Management > root**.

Step 2 In the Sub-Elements tab, select the tenant you want to edit, then click **Edit**.

Step 3 In the **Edit Tenant** dialog box, modify description, then click **OK**. The Level field identifies the tenant's level in the hierarchy and is read-only.

Deleting a Tenant

Note When you delete an organization (such as a tenant, virtual data center, application, or tier), all data contained under the organization is deleted, including sub organizations, compute firewalls, edge firewalls, resource pools, and policies.

Procedure

Step 1 Choose **Tenant Management > root > Sub-Elements**.

Step 2 Select the tenant you want to delete, then click **Delete Tenant**.

Step 3 When prompted, confirm the deletion.

Configuring Virtual Data Centers

Creating a Virtual Data Center

Procedure

Step 1 Choose **Tenant Management > root >** *tenant*, where *tenant* is the location for the new virtual data center.

Step 2 In the General tab, click **Create Virtual Data Center**.

Step 3 In the Create Virtual Data Center dialog box, complete the following fields, then click **OK**:

Field	Description
Name	VDC name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief VDC description. This field can contain between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon.

Editing a Virtual Data Center

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **> Sub-Elements**.

Step 2 In the Sub-Elements tab, select the virtual data center you want to edit, then click **Edit**.

Step 3 In the Edit Virtual Data Center dialog box, modify the description, then click **OK**. The Level field indicates the level of the virtual data center in the hierarchy, and is read-only.

Deleting a Virtual Data Center

Note When you delete a virtual data center, all data contained under the virtual data center is deleted, including sub-organizations, firewalls, resource pools, and policies.

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **> Sub-Elements**, where *tenant* is the tenant with the virtual data center that you want to delete.

Step 2 Select the virtual data center that you want to delete, then click **Delete Virtual Data Center**.

Step 3 When prompted, confirm the deletion.

Configuring Applications

Creating an Application

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* where *vdc* is the location for the new application.

Step 2 In the General tab, click **Create Application**.

Step 3 In the Create Application dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Application name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief application description. This field can be between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon.

Editing an Application

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **>** *virtual-data-center* **> Sub-Elements** , where *virtual-data-center* is the virtual data center with the application that you want to edit.

Step 2 Select the application that you want to edit, then click **Edit**.

Step 3 In the Edit Application dialog box, modify the description as required, then click **OK**. The Level field identifies the level of the application in the hierarchy, and is read-only.

Deleting an Application

Note When you delete an application, all data contained under the application is deleted, including sub-organizations, firewalls, resource pools, and policies.

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **>** *virtual-data-center* **> Sub-Elements**, where *virtual-data-center* is the virtual data center with the application you want to delete.

Step 2 Select the application that you want to delete, then click **Delete Application**.

Step 3 When prompted, confirm the deletion.

Configuring Tiers

Creating a Tier

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application*, where *application* is the location for the new tier.

Step 2 In the General tab, click **Create Tier**.

Step 3 In the Create Tier dialog box, complete the following fields, then click **OK**:

Field	Description
Name	The name of the Tier. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	A description of the Tier. This field can contain between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon.

Editing a Tier

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **>** *virtual-data-center* **>** *application* **>** *tier* where *tier* is the tier you want to edit.

Step 2 In the Properties tab, modify the description as required, then click **Save**.

Deleting a Tier

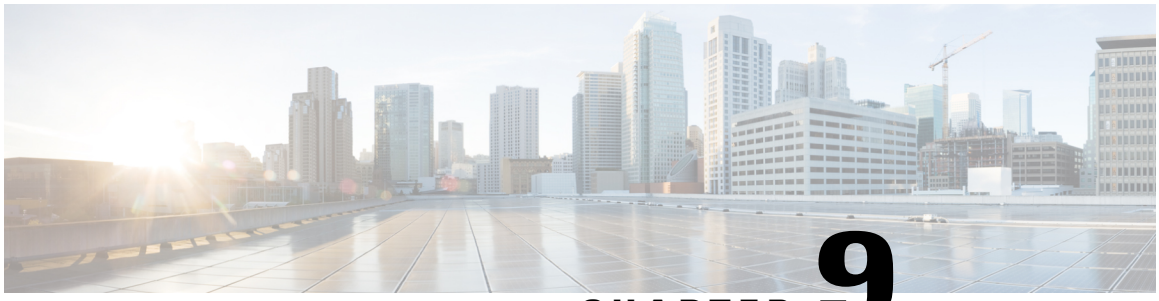
Note When you delete a tier, all data contained under it is also deleted, including sub-organizations, firewalls, resource pools, and policies.

Procedure

Step 1 Choose **Tenant Management > root >** *tenant* **> Sub-Elements**, where *tenant* contains the tier you want to delete.

Step 2 Navigate to the tier you want to delete, select it, then click **Delete Tier**.

Step 3 When prompted, confirm the deletion.



CHAPTER 9

Configuring Service Policies and Profiles

This section includes the following topics:

- Configuring Service Policies, page 77
- Working with Profiles, page 113
- Configuring Security Profiles, page 121
- Configuring Security Policy Attributes, page 125

Configuring Service Policies

The following topics describe concepts and options for configuring service policies and policy sets:

- Configuring ACL Policies and Policy Sets, on page 77
- Configuring Connection Timeout Policies, on page 84
- Configuring DHCP Policies, on page 86
- Configuring IP Audit and IP Audit Signature Policies, on page 89
- Configuring NAT/PAT Policies and Policy Sets, on page 92
- Configuring Packet Inspection Policies, on page 97
- Configuring Routing Policies, on page 98
- Configuring TCP Intercept Policies, on page 99
- Configuring Site-to-Site IPsec VPN Policies, on page 100

Configuring ACL Policies and Policy Sets

The following topics describe how to configure ACL policies and policy sets:

- Adding an ACL Policy, on page 78
- Time Ranges in ACL Policy Rules, on page 82

- Adding an ACL Policy Set, on page 84

Adding an ACL Policy

VNMC enables you to implement access control lists based on the time of day and frequency, or inclusion in a defined group. Benefits of this feature include:

- Providing closer control of access to network resources throughout the day or week.
- Enhancing policy-based routing and queuing functions.
- Automatically rerouting traffic at specific times of the day to ensure cost-effectiveness.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policies**.

Step 2 In the General tab, click **Add ACL Policy**.

Step 3 In the Add ACL Policy dialog box, enter a name and brief description for the policy, then click **Add Rule**.

Step 4 In the Add Rule dialog box, specify the required information as described in Add ACL Policy Rule Dialog Box, on page 78, then click **OK**.

Note All Network Port conditions in a single ACL rule must have the same value selected in the Attribute Value field. For example, you would choose FTP from the Attribute Value drop-down list for all rule conditions that specify the Attribute Name of Network Port.

The Add Rule dialog box contains settings for time rules for ACL policies. For more information about using time ranges with ACL policies, see Time Ranges in ACL Policy Rules, on page 82.

Add ACL Policy Rule Dialog Box

Field	Description
Name	Rule name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	Brief rule description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).

Field	Description
Action to Take	1 Select the action to take if the rule conditions are met: • Drop—Drops traffic or denies access. • Permit—Forwards traffic or allows access. • Reset—Resets the connection. 2 Check the **Log** check box to enable logging.
Condition Match Criteria	Condition Match Options. • Choose match-all for the ACL Policy Rule to match all the conditions (AND). • Choose match-any for the ACL Policy Rule to match any one condition (OR). **Note** If VNMC is installed on Hyper-V Hypervisor, the Condition Match Criteria is disabled. The vZone must match all the conditions.
Src-Dest-Service Tab A rule can have a service condition or a protocol condition, but not both.	
Source Conditions	Source Rule Condition 1 Click **Add**. 2 Enter the required values for following: • Attribute Type **Note** If VNMC is installed on Hyper-V Hypervisor, the VM and User Defined attribute types are not supported. • Attribute Name • Operator • Attribute Value 3 Click **OK**.

Field	Description
Destination Conditions	Destination Rule Condition **1** Click **Add**. **2** Enter the required values for following: • Attribute Type **Note** If VNMC is installed on Hyper-V Hypervisor, the attribute type VM is not supported. • Attribute Name • Operator • Attribute Value **3** Click **OK**.
Service	Service Expression **1** Click **Add**. **2** Enter the required values for following: • Operator • Protocol • Port **3** Click **OK**. **Note** If VNMC is installed on Hyper-V Hypervisor, the Service Condition is disabled.
Protocol Tab	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not Equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.

Field	Description
Ether Type Tab	Specify the encapsulated protocols to be examined for this rule. To examine specific encapsulated protocols: **1** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Greater than, Less than, Member, Not Member, In range, or Not in range. **2** In the Value fields, specify the hexadecimal value, object group, or hexadecimal range.
Time Range Tab	
To apply the rule all the time	Check the **Always** check box.
To apply the rule for a specific time range	**1** Uncheck the **Always** check box. **2** Check the **Range** check box. **3** In the Absolute Start Time fields, provide the start date and time. **4** In the Absolute End Time fields, provide the end date and time.
To apply the rule based on membership in an object group	**1** Uncheck the **Always** check box. **2** Check the **Pattern** check box. **3** From the Operator drop-down list, choose **member (Member of)**. **4** Do any of the following : • From the **Select Object Group** drop-down list, choose an existing object group. • Click **Add Object Group** to create a new object group. • Click the Resolved Object Group link to review or modify the specified object group.

Field	Description
To apply the rule on a periodic basis, with the frequency you specify	1 Uncheck the **Always** check box. 2 Check the **Pattern** check box. 3 From the Operator drop-down list, choose **range (In range)**. 4 In the Begin fields: 1 From the Begin drop-down list, choose the beginning day of the week or the frequency of the time range. 2 Choose the beginning hour and minute, and AM or PM. 5 In the End fields: 1 From the End drop-down list, choose the ending day of the week or frequency. 2 Choose the ending hour and minute, and AM or PM. **Note** If you choose a frequency in the Begin drop-down list, choose the same frequency in the End drop-down list. For example, choose Weekdays from both the Begin and End drop-down lists.
Advanced Tab	Source port attributes that must be matched for the current policy to apply. To add a new source port: 1 Click **Add**. 2 Provide the required information in the following fields, then click **OK**: • Attribute Name • Operator • Attribute Value

Time Ranges in ACL Policy Rules

VNMC enables you to configure time ranges for ACL policy rules in either of the following ways:

- By specifying a time range for the ACL policy rule.
- By associating an ACL object group with the ACL policy rule.

VNMC supports the following types of time ranges:

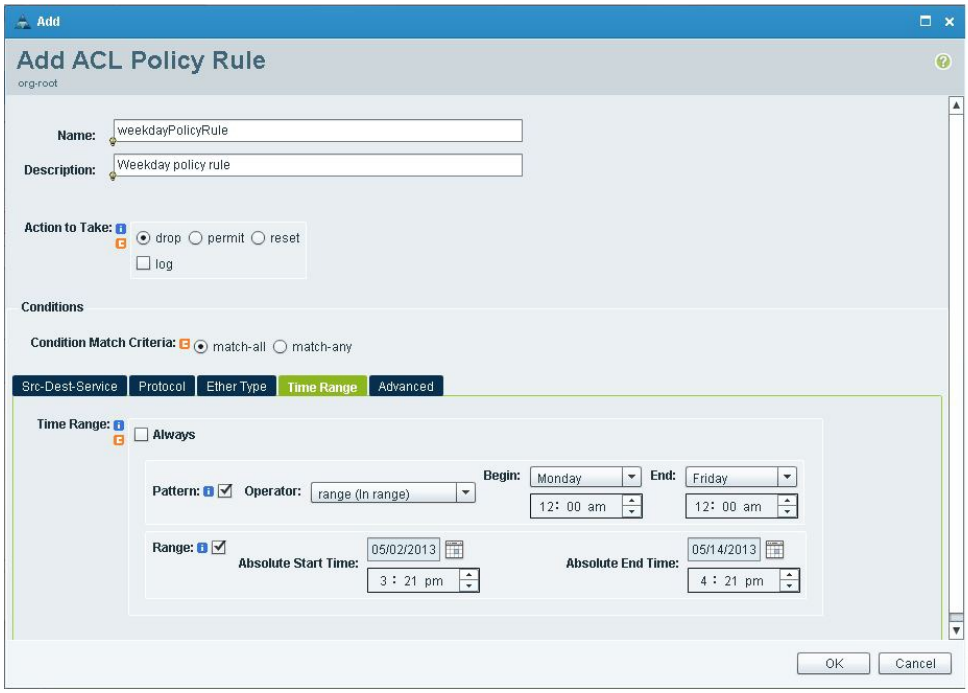
- Periodic—Specified by day-of-week start and end times (such as Sunday to Sunday), or a frequency (such as Daily, Weekdays, or Weekends). Periodic range start and end times also include options for hours and minutes.
- Absolute—Specified by a calendar date and time for start and end times, such as 01 Sep 2013 12:00 AM to 31 Dec 2013 12:00 AM.

For each ACL policy rule, you can have:

- One absolute time range.
- Any number of periodic time ranges, or none.
  - To specify a single periodic time range, add it to an ACL policy rule.
  - To specify multiple periodic time ranges, use an ACL policy object group.

The following figure shows the Time Range fields for an ACL policy rule.

Figure 2: Time Range Fields in an ACL Policy Rule



Adding an ACL Policy Set

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policy Sets**.

Step 2 In the General tab, click **Add ACL Policy Set**.

Step 3 In the Add ACL Policy Set dialog box, enter the required information as described in the following table, then click **OK**:

Field	Description
Name	Policy set name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	Policy set description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Admin State	Administrative state of the policy: enabled or disabled. This field is not available for all policy sets.
Policies	
Add Policy	Click to add a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

Configuring Connection Timeout Policies

VNMC enables you to configure connection timeout policies so that you can establish timeout limits for different traffic types.

After you create a connection timeout policy, you can associate it with an edge security profile. For more information, see Configuring Edge Security Profiles, on page 117.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > Connection Timeout**.

Step 2 In the General tab, click **Add Connection Timeout Policy**.

Step 3 In the Add Connection Timeout Policy dialog box:

a) Enter a policy name and description.

b) Choose whether the administrative status of the policy is to be enabled or disabled.

Step 4 To add a rule to the policy, click **Add Rule**.

Step 5 In the Add Connection Timeout Policy Rule dialog box, provide the information as described in Add Connection Timeout Policy Rule Dialog Box, on page 85.

Add Connection Timeout Policy Rule Dialog Box

Table 6: Add Connection Timeout Policy Rule Dialog Box

Field	Description
Name	Policy name.
Description	Brief policy description.
Action	
Idle TCP	Length of time (in days, hours, minutes, and seconds) a TCP connection can remain idle before it is closed.
Half-Closed	Length of time (in days, hours, minutes, and seconds) a half-closed TCP connection can remain idle before it is freed.
Send Reset To Idle Connection	Check the check box to send a reset to the TCP endpoints when a TCP connection times out.
Idle UDP	Length of time (in days, hours, minutes, and seconds) a UDP connection can remain idle before it closes. The duration must be at least one minute, and the default value is two minutes. Enter 00:00:00:00 to disable timeout.
ICMP	Length of time (in days, hours, minutes, and seconds) an ICMP state can remain idle before it is closed.

Field	Description
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

Configuring DHCP Policies

VNMC enables you to create the following DHCP policies and apply them to edge firewalls:

- DHCP relay server policy
- DHCP server policy

These policies can be authored at the organization level and can be applied only to the inside interface of an edge firewall. When they are applied, DHCP policies allow the edge firewall to act either as a DHCP server or a DHCP relay for all VMs in the inside network.

You can apply only one DHCP server or relay profile at a time to the inside interface of the edge firewall.

For more information, see the following topics:

- Adding a DHCP Relay Server, on page 86
- Configuring a DHCP Relay Policy, on page 87
- Configuring a DHCP Server Policy, on page 88

Adding a DHCP Relay Server

DHCP relay servers are used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. In contrast to IP router forwarding, where IP datagrams are switched between networks, DHCP relay servers receive DHCP messages and then generate a new message to send out on a different interface.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay Server**.

Step 2 In the General tab, click **Add DHCP Relay Server**.

Step 3 In the New DHCP Relay Server dialog box, provide the information described in the Add DHCP Relay Server Dialog Box, on page 87, then click **OK**.

Add DHCP Relay Server Dialog Box

Field	Description
Name	Relay server name.
Description	Brief description of the relay server.
Relay Server IP	IP address of the relay server.
Interface Name	Interface to use to reach the relay server.

Configuring a DHCP Relay Policy

VNMC enables you to associate a DHCP relay server with a DHCP relay policy, as described in this procedure.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay**.

Step 2 In the General tab, click **Add DHCP Relay Policy**.

Step 3 In the New DHCP Relay Policy dialog box, provide the information described in Add DHCP Relay Policy Dialog Box, on page 87, then click **OK**.

Add DHCP Relay Policy Dialog Box

Name	Description
Name	Policy name.
Description	Brief policy description.
DHCP Relay Server Assignment	Assign a DHCP relay server in one of the following ways: • Click **Add DHCP Relay Server** to add a new DHCP relay server. • In the Available Relay Servers list, select one of the available relay servers and move it to the Assigned Relay Servers list You must assign at least one DHCP relay server to the policy.

Configuring a DHCP Server Policy

A DHCP server policy enables you to define the characteristics of the policy, such as ping and lease timeouts, IP address range, and DNS and WINS settings.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Server**.

Step 2 In the General tab, click **Add DHCP Server Policy**.

Step 3 In the New DHCP Server Policy dialog box, provide the information as described in Add DHCP Server Policy Dialog Box, on page 88, then click **OK**.

Add DHCP Server Policy Dialog Box

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Ping Timeout (Milliseconds)	Amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The valid range is 10 to 10000 milliseconds.
Lease Timeout	Amount of time (in days, hour, minutes, and seconds) that the DHCP server allocates an IP address to a DHCP client before reclaiming and then reallocating it to another client. The default value is 00:01:00:00 (one hour).
Edge Firewall Interface Using the DHCP Client for DHCP Server Auto Configuration	To enable DHCP server automatic configuration, enter the name of the edge firewall interface that uses the DHCP client. For ASA 1000V instances, this interface is always an outside interface. Leaving this field empty indicates that the automatic configuration feature is disabled.
Policies Tab	

Field	Description
DNS Settings	DNS settings used by the edge firewall when configuring DHCP clients. To add a new entry, click **Add DNS Setting** and add the required information.
WINS Servers	Windows Internet Naming Service (WINS) name servers that are available to DHCP clients. To add a new WINS server, click **Add WINS Server** and enter the WINS server IP address. WINS servers are listed in the order of preference, with the most preferred WINS server at the top. Select an entry in the table, and then use the arrows above the table to change server priority.
IP Address Range	Enter the following information for the DHCP address pool: • Start IP Address—Beginning IP address of the pool. • End IP Address—Ending IP address of the pool. • Subnet Mask—Subnet mask to apply to the address pool.

Configuring IP Audit and IP Audit Signature Policies

The IP audit feature provides basic Intrusion Prevention System (IPS) support for ASA 1000V instances. VNMC supports a basic list of signatures, and enables you to configure policies that specify one or more actions to apply to traffic that matches a signature.

The following IP audit policies are available:

- Audit policies
- Signature policies

When you associate an IP audit policy with a device, the policy is applied to all traffic on the outside interface of the device.

The following topics describe how to configure these policies.

Configuring IP Audit Policies

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > IP Audit > Audit Policies**.

Step 2 In the General tab, click **Add IP Audit Policy**.

Step 3 In the Add IP Audit Policy dialog box provide the following information:

- Policy name
- Policy description
- In the Admin State field, choose whether the administrative state of the policy is to be enabled or disabled.

Step 4 To add a rule to the policy, click **Add Rule**.

Step 5 In the Add IP Audit Policy Rule dialog box, provide the information as described in Add IP Audit Policy Rule Dialog Box, on page 90, then click **OK** in the open dialog boxes.

Add IP Audit Policy Rule Dialog Box

Table 7: IP Audit Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Attack-Class Action	Check the check boxes of the actions to take for signature type Attack if the conditions of the rule are met: • Log—Send a message indicating that a packet matched the signature. • Drop—Drop the packet. • Reset Flow—Drop the packet and reset the connection.

Field	Description
Information-Class Action	Check the check boxes of the actions to take for signature type Informational if the conditions of the rule are met: • Log—Send a message indicating that a packet matched the signature. • Drop—Drop the packet. • Reset Flow—Drop the packet and reset the connection.
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

Configuring IP Audit Signature Policies

An IP audit signature policy identifies the signatures that are enabled and disabled. By default, all signatures are enabled. You can disable a signature when legitimate traffic matches the signature in most situations, resulting in false alarms. However, disabling the signature is performed at a global level, meaning that no traffic will trigger the signature (even bad traffic) when it is disabled.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > IP Audit > Signature Policies**.

Step 2 In the General tab, click **Add IP Audit Signature Policy**.

Step 3 In the Add IP Audit Signature Policy dialog box, enter a name and description for the policy.

Step 4 In the Signatures area, move signatures between the Enabled Signatures and Disabled Signatures lists as required.

Note We recommend that you do not disable signatures unless you are sure you understand the consequences of doing so.

You can view additional information about a signature by selecting the required signature and clicking **Properties**.

Step 5 After you have made all adjustments, click **OK**.

Configuring NAT/PAT Policies and Policy Sets

VNMC supports Network Address Translation (NAT) and Port Address Translation (PAT) policies for controlling address translation in the deployed network. These policies support both static and dynamic translation of IP addresses and ports.

VNMC enables you to configure the following policy items:

- NAT policy—Can contain multiple rules, which are evaluated sequentially until a match is found.
- NAT policy set—Group of NAT policies that can be associated with an edge security profile. When the profile is applied, the NAT policies are applied only to ingress traffic.
- PAT policy—Supports source dynamic and destination static interface PAT on edge firewalls.

The following topics describe how to configure NAT and PAT policies, and NAT policy sets.

Configuring NAT/PAT Policies

This procedure describes how to configure NAT/PAT policies with VNMC.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.

Step 2 In the General tab, click **Add NAT Policy**.

Step 3 In the Add NAT Policy dialog box, enter a name and description for the policy.

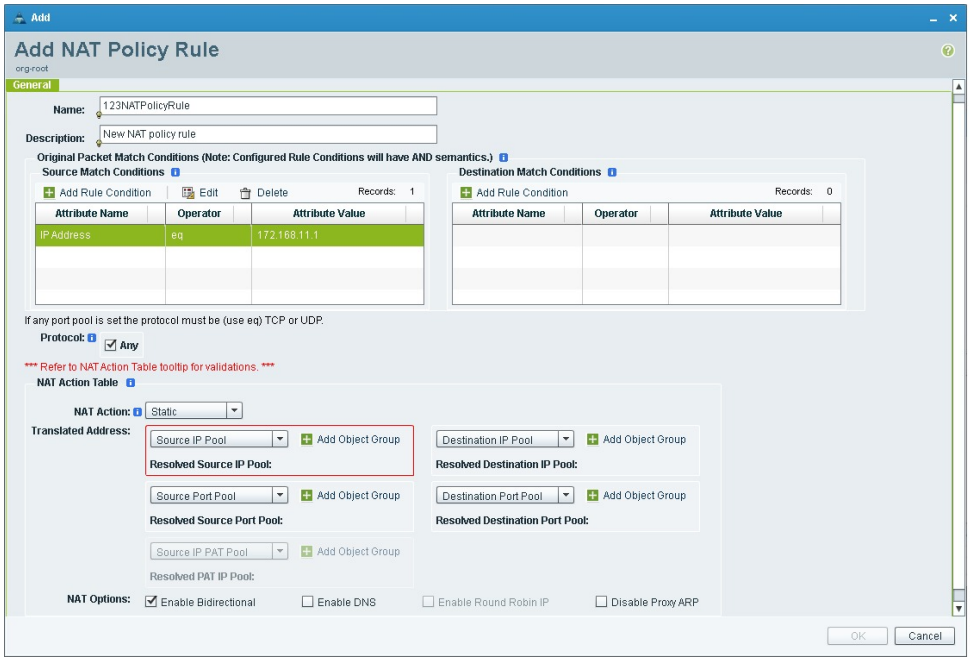
Step 4 In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.

Step 5 To add a rule to the policy, click **Add Rule**.

Step 6 In the Add NAT Policy Rule dialog box, provide the information as described in Add NAT Policy Rule Dialog Box, on page 93, then click **OK** in the open dialog boxes.

Add NAT Policy Rule Dialog Box

Figure 3: Add NAT Policy Rule Dialog Box



Add NAT Policy Rule Dialog Box

Add NAT Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Original Packet Match Conditions	
Source Match Conditions	Source attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available source attributes are IP Address and Network Port.

Field	Description
Destination Match Conditions	Destination attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available destination attributes are IP Address and Network Port.
Protocol	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
NAT Action Table	
NAT Action	From the drop-down list, choose the required translation option: Static or Dynamic.
Translated Address	Identify a translated address pool for each original packet match condition from the following options: • Source IP Pool • Source Port Pool • Source IP PAT Pool • Destination IP Pool • Destination Port Pool For example, if you specify a source IP address match condition, you must identify a Source IP Pool object group. Similarly, a destination network port match requires a Destination Port Pool object group. The Source IP PAT Pool option is available only if you choose dynamic translation. Click **Add Object Group** to add object groups for the translation actions.

Field	Description
NAT Options	Check and uncheck the check boxes as required: • Enable Bidirectional--Check the check box for connections to be initiated bidirectionally; that is, both to and from the host. Available only for static address translation. • Enable DNS--Check the check box to enable DNS for NAT. • Enable Round Robin IP--Check the check box to allocate IP addresses on a round-robin basis. Available only for dynamic address translation. • Disable Proxy ARP—Check the check box to disable proxy ARP. Available only for static address translation.

Configuring NAT Policy Sets

Policy sets enable you to group multiple policies of the same type (such as NAT, ACL, or Interface) for inclusion in a profile. NAT policy sets are groups of NAT policies that can be associated with an edge security profile.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policy Sets**.

Step 2 In the General tab, click **Add NAT Policy Set**.

Step 3 In the Add NAT Policy Set dialog box, enter a name and description for the policy set.

Step 4 In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.

Step 5 In the Policies area, select the policies to include in this policy set:

a) In the Available list, select one or more policies and move them to the Assigned list.

b) Adjust the priority of the assigned policies by using the arrow keys above the list.

c) If required, click **Add NAT Policy** to add a new policy and include it in the Assigned list.
For information on configuring a NAT policy, see Configuring NAT/PAT Policies, on page 92.

Step 6 Click **OK**.

Configuring PAT for Edge Firewalls

VNMC enables you to configure source and destination interface PAT for edge firewalls, such as the ASA 1000V. For more information, see the following topics.

Configuring Source Dynamic Interface PAT

VNMC enables you to configure source dynamic interface PAT for edge firewalls, such as ASA 1000Vs.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.

Step 2 In the General tab, click **Add NAT Policy**.

Step 3 In the Add NAT Policy dialog box, enter a name and description for the policy.

Step 4 In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.

Step 5 Click **Add Rule** to add a rule to this policy.

Step 6 In the Add NAT Policy Rule dialog box, provide the information described in Add NAT Policy Rule Dialog Box, on page 93 with the following specific settings, then click **OK**:

a) From the NAT Action drop-down list, choose **Dynamic**.

b) In the Translated Address area, add a Source IP Pool object group that contains the ASA 1000V outside interface IP address.

Step 7 Click **OK**.

Configuring Destination Static Interface PAT

VNMC enables you to configure destination static interface PAT for edge firewalls, such as ASA 1000Vs, as described in the following procedure.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.

Step 2 In the General tab, click **Add NAT Policy**.

Step 3 In the Add NAT Policy dialog box, enter a name and description for the policy.

Step 4 In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.

Step 5 Click **Add Rule** to add a rule to this policy.

Step 6 In the Add NAT Policy Rule dialog box, enter the IP address of the ASA 1000V outside interface as a rule condition for Destination Match Conditions.

Step 7 Configure other options in the Add NAT Policy Rule dialog box as described in Add NAT Policy Rule Dialog Box, on page 93, then click **OK**.

Note If any of the IP address fields includes a range that starts or ends with the IP address of the outside interface of the ASA 1000V, an error message will be displayed that identifies an overlap with the ASA 1000V interface IP address.

Step 8 Click **OK**.

Configuring Packet Inspection Policies

VNMC enables you to configure policies for application-layer protocol inspection. Inspection is required for services that embed IP addressing information in the user data packet, or that open secondary channels on dynamically assigned ports. When inspection is configured, the end device performs a deep packet inspection instead of quickly passing the packet on. As a result, inspection can affect overall device throughput.

Protocols Supported for Packet Inspection Policies, on page 97 lists the application-layer protocols supported by VNMC.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > Packet Inspection**.

Step 2 In the General tab, click **Add Packet Inspection Policy**.

Step 3 In the Add Packet Inspection Policy dialog box, enter a name and description for the policy.

Step 4 In the Admin State field, indicate whether the administrative status of the policy is enabled or disabled.

Step 5 To add a rule to the policy, click **Add Rule**.

Step 6 In the Add Packet Inspection Policy Rule Dialog box, provide the information as described in Add Packet Inspection Policy Rule Dialog Box, on page 98, then click **OK**.

Protocols Supported for Packet Inspection Policies

Protocols Supported for Packet Inspection Policies

CTIQBE	ICMP	PPTP	SQLNet
DCE/RPC	ICMP Error	RSH	SunRPC
DNS	ILS	RSTP	TFTP
FTP	IP Options	SIP	WAAS
H323 H225	IPsec Pass-Through	Skinny	XDMCP
H323 RAS	MGCP	SMTP	
HTTP	NetBIOS	SNMP	

Add Packet Inspection Policy Rule Dialog Box

Table 8: Add Packet Inspection Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Action	In the Enable Inspection fields, check the check boxes of protocols to be inspected if the rule conditions are met.
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

Configuring Routing Policies

VNMC enables you to use routing policies to configure static routes for managed endpoints on an edge firewall.

Note You can configure only inside and outside interfaces on edge firewalls by using VNMC. Use the CLI to configure routes on the edge firewall management interface.

After you configure a static route routing policy, you can implement the policy by:

- Including the routing policy in an edge device profile.
- Applying the edge device profile to an edge firewall that has managed endpoints.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > Routing**.

Step 2 In the General tab, click **Add Routing Policy**.

Step 3 In the Add Routing Policy dialog box, enter a name and brief description for the routing policy.

Step 4 To add a new static route, click **Add Static Route**.

Step 5 In the Add Static Route dialog box, enter the following information:

a) In the Destination Network fields, enter the IP route prefix and prefix mask for the destination.

b) In the Forwarding (Next Hop) fields, enter the IP address of the next hop that can be used to reach the destination network.

Note The Forwarding Interface field applies only to ASA 1000V data interfaces. Use the CLI to configure routes on the ASA 1000V management interface.

c) (Optional) In the Distance Metric field, enter the distance metric.

Step 6 Click **OK**.

Configuring TCP Intercept Policies

VNMC enables you to configure TCP intercept policies that you can then associate with an edge security profile. TCP intercept policies that you associate with a device via an edge security profile are applied to all traffic on the outside interface of the device.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > TCP Intercept**.

Step 2 In the General tab, click **Add TCP Intercept Policy**.

Step 3 In the Add TCP Intercept Policy dialog box, enter a name and brief description for the policy.

Step 4 In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.

Step 5 To add a rule to the policy, click **Add Rule**.

Step 6 In the Add TCP Intercept Policy Rule dialog box, provide the information as described in Add TCP Intercept Policy Rule Dialog Box, on page 99.

Add TCP Intercept Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Maximum Number of Embryonic TCP Connections (0-65535)	Number of embryonic TCP connections allowed overall and per client: **1** In the Total field, enter the maximum number of embryonic TCP connections allowed. **2** In the client field, enter the maximum number of embryonic TCP connections allowed per client. The default value 0 (zero) indicates unlimited connections.
Protocol	Not available for configuration.

Field	Description
Source Conditions	Not available for configuration.
Destination Conditions	Not available for configuration.

Configuring Site-to-Site IPsec VPN Policies

VNMC enables you to configure site-to-site IPsec VPNs. In addition, you can configure a crypto map policy and attach it to an edge profile. For ease of configuration and to keep logical IPsec entities separate, configuration is divided into the following sections:

- Configuring Crypto Map Policies
- Configuring IKE Policies
- Configuring Interface Policy Sets
- Configuring IPsec Policies
- Configuring Peer Authentication Policies
- Configuring VPN Device Policies

To access VPN policies, choose **Policy Management > Service Policies > root > Policies > VPN.**

Configuring Crypto Map Policies

VNMC enables you to create crypto map policies that include:

- Rules for source and destination conditions.
- IP Security (IPsec) options, including an IPsec policy.
- Internet Key Exchange (IKE) options, including a peer device.

Crypto map policies are applied to interfaces by means of their inclusion in interface policy sets and edge security policies.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > Crypto Map Policies**.

Step 2 In the General tab, click **Add Crypto Map Policy**.

Step 3 In the Add Crypto Map Policy dialog box, provide the information as described in Add Crypto Map Policy Dialog Box, on page 101, then click **OK**.

Step 4 To add a policy rule, click **Add Rule** in the General tab and provide the required information as described in Add Crypto Map Policy Rule Dialog Box, on page 103.

Add Crypto Map Policy Dialog Box

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Admin State	Whether the administrative status of the policy is enabled or disabled.
Rule Table	
Add Rule	Click **Add Rule** to add a new rule to the current policy.
IPsec Settings Tab	
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that a security association (SA) lives before expiring.
SA Lifetime Traffic (KB)	Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before that association expires.
Enable Perfect Forwarding Secrecy	Whether or not Perfect Forward Secrecy (PFS) is enabled. PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.
Diffie-Hellman Group	Available if PFS is enabled. Choose the Diffie-Hellman (DH) group for this policy: • Group 1--The 768-bit DH group. • Group 2--The 1024-bit DH group. • Group 5--The 1536-bit DH group.
IPsec Policies	The IPsec policy that applies to the current policy. Select an existing IPsec policy or click **Add IPsec Policy** to create a new policy.

Field	Description
Peer Device	Peer device. Choose an existing peer or click **Add Peer Device** to add a new peer. In the Add Peer Device dialog box, enter the peer device IP address or hostname.
Other Settings Tab	
Enable NAT Traversal	Whether or not IPsec peers can establish a connection through a NAT device.
Enable Reverse Route Injection	Whether or not static routes are automatically added to the routing table and then announced to neighbors on the private network.
Connection Type	Connection type for this policy: • Answer-Only--Responds only to inbound IKE connections during the initial proprietary exchange to determine the appropriate peer to which to connect. • Bidirectional--Accepts and originates connections based on this policy. • Originate-Only--Initiates the first proprietary exchange to determine the appropriate peer to which to connect.
Negotiation Mode	Mode to use for exchanging key information and setting up SAs: • Aggressive Mode--Faster mode, using fewer packets and exchanges, but does not protect the identity of the communicating parties. • Main Mode--Slower mode, using more packets and exchanges, but protects the identities of the communicating parties.
DH Group for Aggressive Mode	DH group to use when in aggressive mode: Group 1, Group 2, or Group 5.

Add Crypto Map Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
VPN Action	Action to take based on this rule: Permit or Deny.
Protocol	Protocols to examine for this rule: • To examine all protocols, check the **Any** check box. • To examine specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
Source Conditions	Source attributes that must be matched for the rule to apply. To add a new condition, click **Add Rule Condition**. Available source attributes are IP Address and Network Port.
Destination Conditions	Destination attributes that must be matched for the rule to apply. To add a new condition, click **Add Rule Condition**. Available destination attributes are IP Address and Network Port.

Configuring IKE Policies

The Internet Key Exchange (IKE) protocol is a hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. The initial IKE implementation used the IPsec protocol, but IKE can be used with other protocols. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates the IPsec Security Associations (SAs).

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > IKE Policies**.

Step 2 In the General tab, click **Add IKE Policy**.

Step 3 In the Add IKE Policy dialog box, enter a name and description for the policy.

Step 4 Configure either an IKE V1 or IKE V2 policy:

- IKE V1 Policy
  1. Click **Add IKE V1 Policy**.
  2. In the Add IKE V1 Policy dialog box, provide the information described in IKE V1 Policy Dialog Box, on page 104, then click **OK**.
- IKE V2 Policy
  1. Click **Add IKE V2 Policy**.
  2. In the Add IKE V2 Policy dialog box, provide the information described in IKE V2 Policy Dialog Box, on page 104, then click **OK**.

Step 5 Click **OK**.

IKE V1 Policy Dialog Box

Field	Description
DH Group	Diffie-Hellman group: Group 1, Group 2, or Group 5.
Encryption	Encryption method: 3DES, AES, AES-192, AES-256, or DES.
Hash	Hash algorithm: MD5 or SHA.
Authentication	Authentication method is Preshared key.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring.

IKE V2 Policy Dialog Box

Field	Description
DH Group	Diffie-Hellman group: Group 1, Group 2, Group 5, or Group 14.

Field	Description
Encryption	Encryption method: 3DES, AES, AES-192, AES-256, or DES.
Hash	Hash integrity algorithm: MD5, SHA, SHA256, SHA384, or SHA512.
Pseudo Random Function Hash	Pseudo-random function (PRF) has algorithm: MD5, SHA, SHA256, SHA384, or SHA512.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring.

Configuring Interface Policy Sets

Interface policy sets enable you to group multiple policies for inclusion in an edge security profile.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > Interface Policy Sets**.

Step 2 In the General tab, click **Add Interface Policy Set**.

Step 3 In the Add Interface Policy Set dialog box, provide the information as described in Add Interface Policy Set Dialog Box, on page 105, then click **OK**.

Add Interface Policy Set Dialog Box

General Tab

Field	Description
Name	Policy set name.
Description	Brief description of the policy set.
Admin State	Administrative state of the policy set: enabled or disabled.
Policies Area	
Add Crypto Map Policy	Click to add a new policy.

Field	Description
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

Domain Settings Tab

Field	Description
Enable IKE (Must check at least one)	Check the appropriate check box to specify IKE V1 or IKE V2.
Enable IPsec Pre-fragmentation	Check the check box to fragment packets before encryption. Pre-fragmentation minimizes post-fragmentation (fragmentation after encryption) and the resulting reassembly before decryption, thereby improving performance.
Do Not Fragment	Available only if the Enable IPsec Pre-fragmentation check box is checked. From the drop-down list, choose the action to take with the Don't Fragment (DF) bit in the encapsulated header: • Clear • Copy • Set

Configuring IPsec Policies

IPsec policies define the IPsec policy objects used to create a secure IPsec tunnel for a VPN.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > IPsec Policies**.

Step 2 In the General tab, click **Add IPsec Policy**.

Step 3 In the Add IPsec Policy dialog box, enter a name and description for the policy.

You must configure ethier an IKE V1 or IKE V2 proposal for an IPsec policy.

Step 4 To configure an IKE V1 proposal:

a) In the IKE v1 Proposal Table area, click **Add IPsec IKEv1 Proposal**.

b) In the IPsec IKEv1 Proposal dialog box, provide the information described in IPsec IKEv1 Proposal Dialog Box, on page 107, then click **OK**.

Step 5 To configure an IKE V2 proposal:

a) In the IKE v2 Proposal Table area, click **Add IPsec IKE v2 Proposal**.

b) In the IPsec IKEv2 Proposal dialog box, provide the information described in IPsec IKEv2 Proposal Dialog Box, on page 108, then click **OK**.

Step 6 Click **OK** to save the policy.

IPsec IKEv1 Proposal Dialog Box

Field	Description
Mode	Mode in which the IPsec tunnel operates. In Tunnel mode, the IPsec tunnel encapsulates the entire IP packet.
ESP Encryption	Encapsulating Security Protocol (ESP) encryption method: • 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys. • AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys. • AES-192—Encrypts according to the AES using 192-bit keys. • AES-256—Encrypts according to the AES using 256-bit keys. • DES—Encrypts according to the DES using 56-bit keys. • Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only.

Field	Description
ESP Authentication	Hash authentication algorithm: • MD5—Produces a 128-bit digest. • Null—Does not perform authentication. • SHA—Produces a 160-bit digest.

IPsec IKEv2 Proposal Dialog Box

Field	Description
ESP Encryption Algorithm Table	To add an ESP encryption method: 1 Click **Add ESP Encryption Algorithm**. 2 From the ESP Encryption drop-down list, choose the encryption method: • 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys. • AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys. • AES-192—Encrypts according to the AES using 192-bit keys. • AES-256—Encrypts according to the AES using 256-bit keys. • DES—Encrypts according to the DES using 56-bit keys. • Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only.

Field	Description
Integrity Algorithm Table	To add an integrity algorithm: 1 Click **Add Integrity Algorithm**. 2 From the Integrity Algorithm drop-down list, choose the authentication algorithm: • MD5—Produces a 128-bit digest. • Null—Does not perform authentication. • SHA—Produces a 160-bit digest.

Configuring Peer Authentication Policies

Use a peer authentication policy to define the method used to authenticate a peer.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > Peer Authentication**.

Step 2 In the General tab, click **Add Peer Authentication Policy**.

Step 3 In the Add Peer Authentication Policy dialog box, enter a name and description for the policy.

Step 4 Click **Add Policy to Authenticate Peer**.

Step 5 In the Add Policy to Authenticate Peer dialog box, provide the information described in Add Policy to Authenticate Peer Dialog Box, on page 109, then click **OK**.

Step 6 Click **OK** to save the policy.

Add Policy to Authenticate Peer Dialog Box

Field	Description
Peer Device (Unique)	Unique IP address or hostname of the peer.
IKEv1 Area	
Local	Preshared key.
Confirm	Preshared key for confirmation.
Set	Whether or not the preshared key has been set and is properly configured (read-only).
IKEv2 Area	

Field	Description
Local	Local preshared key.
Confirm	Local preshared key for confirmation.
Set	Whether or not the local preshared key has been set and is properly configured (read-only).
Remote	Remote preshared key.
Confirm	Remote preshared key for confirmation.
Set	Whether or not the remote preshared key has been set and is properly configured (read-only).

Configuring VPN Device Policies

A VPN device policy enables you to specify VPN global settings, such as:

- IKE policy
- IKE global settings
- IPsec global settings
- Peer authentication policy

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > VPN Device Policies**.

Step 2 In the General tab, click **Add VPN Device Policy**.

Step 3 In the Add VPN Device Policy dialog box, provide the information as described in Add VPN Device Policy Dialog Box, on page 111.

Step 4 As needed, provide the information described in the following tables:

- Configuring IKE Policies, on page 103
- Configuring Peer Authentication Policies, on page 109

Step 5 Click **OK** to create the policy.

Add VPN Device Policy Dialog Box

General Tab

Note A VPN device policy requires both an IKE policy and a peer authentication policy.

Field	Description
Name	Policy name.
Description	Brief policy description.
IKE Policy	Choose an existing policy from the drop-down list, or click **Add IKE Policy** to add a new policy.
Peer Authentication Policy	Choose an existing policy from the drop-down list, or click **Add Peer Authentication Policy** to add a new policy.

IKE Settings Tab

Field	Description
Enable IPsec over TCP	Whether or not IPsec traffic is allowed over TCP. If IPsec over TCP is enabled, this method takes precedence over all other connection methods.
Send Disconnect Notification	Whether or not clients are notified that sessions will be disconnected.
Allow Inbound Aggressive Mode	Whether or not inbound aggressive mode is permitted.
Wait for Termination before Rebooting	Whether or not a reboot can occur only when all active sessions have terminated voluntarily.
Threshold for Cookie Challenge (0-100 Percent)	Percentage of the maximum number of allowed Security Associations (SAs) that can be in-negotiation (open) before cookie challenges are issued for future SA negotiations.
Negotiation Threshold for Maximum SAs (0-100 Percent)	Percentage of the maximum number of allowed SAs that can be in-negotiation before additional connections are denied. The default value is 100 percent.

Field	Description
IKE Identity	Phase 2 identification method: • Automatic--Determines ISAKMP negotiation by connection type: ◦ IP address for a preshared key. ◦ Cert DN for certificate authentication. • IP Address--IP address of the host exchanging ISAKMP identity information. • Hostname--Fully qualified domain name of the host exchanging ISAKMP identity information. • Key ID--String used by the remote peer to look up the preshared key.
Key for IKE Identity	The key to use for IKE identify if the IKE identification method is Key ID.
NAT Traversal	Whether or not IPsec peers can establish a connection through a NAT device.
Keep-Alive Time for NAT Traversal	Length of time (in hours, minutes, and seconds) that a tunnel can exist with no activity before the device sends keepalive messages to the peer. Values range from 10 to 3600 seconds, with a default of 20 seconds.
IKE Version 2 Maximum Security Associations	Whether or not the total number of IKE V2 SAs on the node can be set.
Maximum number of SA	Maximum number of SA connections allowed.
IKE V1 over TCP Port Table	1 Click **Add IKE V1 Over TCP Port** to add a new port. 2 In the Port field, enter the TCP port to use for IKE V1.

IPsec Settings Tab

Field	Description
Anti Replay	Whether or not SA anti-replay is enabled.

Field	Description
Anti Replay Window Size	Window size to use to track and prevent duplication of packets. Using a larger window size allows the decryptor to track more packets.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA can live before expiring.
SA Lifetime Volume (KB)	Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before the association expires.

Working with Profiles

A profile is a collection of policies. By creating a profile with policies that you select, and then applying that profile to multiple objects, such as edge firewalls, you can ensure that those objects have consistent policies.

A device must be registered to VNMC before you can apply a profile to it.

VNMC enables you to create and apply the following types of profiles:

- Compute security profiles—Compute firewall profiles that include ACL policies and user-defined attributes.
- Edge device profiles—Edge firewall profiles that include routing, VPN, DHCP, and IP Audit policies.
- Edge security profiles—Edge firewall profiles that include access and threat mitigation policies.

The following topics describe how to configure and apply profiles.

Configuring Compute Security Profiles

VNMC enables you to create compute security profiles at the root or tenant level. Creating a compute security profile at the root level enables you to apply the same profile to multiple tenants.

Procedure

Step 1 Choose **Policy Management > Service Profiles > root > Compute Firewall > Compute Security Profiles**.

Step 2 In the General tab, click **Add Compute Security Profile**.

Step 3 In the Add Compute Security Profile dialog box, provide the information as described in Add Compute Security Profile Dialog Box, on page 114, then click **OK**.

Add Compute Security Profile Dialog Box

General Tab

Field	Description
Name	Profile name. This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description	Brief profile description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Policy Set	Drop-down list of policy sets.
Add ACL Policy Set	Click the link to add an ACL policy set.
Resolved Policy Set	Click the link to edit the resolved policy set.
Resolved Policies Area	
(Un)assign Policy	Click the link to assign or unassign a policy.
Name	Rule name.
Source Condition	Source condition for the rule.
Destination Condition	Destination condition for the rule.
Service/Protocol	Service or protocol to which the rule applies.
EtherType	Encapsulated protocol to which the rule applies.
Action	Action to take if the rule conditions are met.
Description	Rule description.

Attributes Tab

Note The Attributes tab is not available for VNMC installed on Hyper-V Hypervisor.

Field	Description
Add User Defined Attribute	Opens a dialog box for adding an attribute.
Name	Attribute name.
Value	Attribute value.

Verifying Compute Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for compute firewalls.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.

Step 2 In the Compute Security Profiles tab, select the required policy, then click **Show Resolved Policies**.

Step 3 In the Edit dialog box, click the required policy in the Resolved Policies table to view the policy details, such as source and destination conditions.

Step 4 To modify a policy, in the Policy Set area, either choose a different policy from the drop-down list, or click **Add ACL Policy Set** to configure a new policy.

Step 5 Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.

Configuring Edge Device Profiles

Edge device profiles contain the following policies in addition to a timeout value for address translation:

- DHCP
- IP audit signature
- Routing
- VPN device

You can create an edge device profile at any level of the organization hierarchy (root, tenant, virtual data center (VDC), app, or tier). Creating an edge device profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

Procedure

Step 1 Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Device Profiles**.

Step 2 In the General tab, click **Add Edge Device Profile**.

Step 3 In the Add Edge Device Profile dialog box, enter the information as described in Edge Device Profile Dialog Box, on page 116, then click **OK**.

Edge Device Profile Dialog Box

Field	Description
Toolbar	
Clone	Clones the current profile.
General Tab	
Name	Profile name.
Description	Brief profile description.
Policies Tab	
Routing Policy	Choose an existing policy or click **Add Routing Policy** to add a new policy. Click the Resolved Policy link to review or modify the assigned policy.
IP Audit Signature Policy	Choose an existing policy or click **Add IP Audit Signature Policy** to add a new policy. Click the Resolved Policy link to review or modify the assigned policy.
VPN Device Policy	Choose an existing policy or click **Add VPN Device Policy** to add a new policy. Click the Resolved Policy link to review or modify the assigned policy.
Address Translations Timeout	Length of time (in days, hours, minutes, and seconds) that a translation can remain unused before it expires.
DHCP Policy Table	
Edge DHCP Policy	Click to add a new DHCP policy.

Field	Description
Type	Type of DHCP service: relay or server.
Interface Name	Interface to which the DHCP policy is applied.
Server/Relay Policy	DHCP policy name.

Events Tab

Field	Description
ID	Unique event identifier.
User	One of the following user types: • admin • internal
Created at	Date and time at which the fault occurred.
Cause	Unique identifier associated with the event cause.
Description	Event description.

Configuring Edge Security Profiles

Edge security profiles can include any of the following:

- ACL policy sets (ingress and egress)
- Connection timeout policies
- IP audit policies
- NAT policy sets
- Packet inspection policies
- TCP intercept policies
- VPN interface policy sets

You can create an edge security profile at any level of the organizational hierarchy (root, tenant, VDC, app, or tier). Creating an edge security profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

Procedure

Step 1 Choose **Policy Management > Service Profiles > Edge Firewall > Edge Security Profiles**.

Step 2 In the General tab, click **Add Edge Security Profile**.

Step 3 In the Add Edge Security Profile dialog box provide the information as described in Add Edge Security Profile Dialog Box, on page 118.

Add Edge Security Profile Dialog Box

Field	Description
General Tab	
Name	Profile name.
Description	Brief profile description.
Ingress Tab	
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Ingress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
Egress Tab	
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Egress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
NAT Tab	
Policy Set	Choose an existing policy set or click **Add NAT Policy Set** to add a new policy set. Click the **Resolved NAT Policy Set** link to modify the assigned policy set.

Field	Description
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
VPN Tab	
Policy Set	Choose an existing policy set or click **Add Interface Policy Set** to add a new policy set. Click the **Resolved VPN Interface Policy Set** link to modify the assigned policy set.
Advanced Tab	
Packet Inspection Policy	Choose an existing policy or click **Add Packet Inspection Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
Connection Timeout Policy	Choose an existing policy or click **Add Connection Timeout Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
TCP Intercept Policy	Choose an existing policy or click **Add TCP Intercept Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
IP Audit Policy	Choose an existing policy or click **Add IP Audit Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.

Applying an Edge Device Profile

After you have created an edge device profile, you can apply the profile to multiple edge firewalls to ensure consistent policies across the firewalls.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
Step 2 In the General tab, click **Select** in the Edge Device Profile field.
Step 3 In the Select Edge Device Profile dialog box, select the required profile, then click **OK**.
Step 4 Click **Save**.

Applying an Edge Security Profile

After you have created an edge security profile, you can apply it to edge firewall instances to ensure consistent policies on the interfaces.

Note Edge security profiles can be applied only on outside interfaces of edge firewalls.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
Step 2 In the Interfaces table, select the required outside interface, then click **Edit**.
Step 3 In the Edit dialog box, click **Select** in the Edge Security Profile field.
Step 4 In the Select Edge Security Profile dialog box, select the required profile, then click **OK**.
Step 5 Click **OK** in the open dialog boxes, then click **Save**.

Verifying Edge Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for edge firewalls.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
Step 2 In the Edge Security Profiles tab, select the required policy, then click **Show Resolved Policies**.
Step 3 To view policy or policy set details, use the tabs in the Edit dialog box to navigate to the required policy or policy set, then click the required policy or policy set in Resolved field
Step 4 To use a different policy or policy set, navigate to the required policy or policy set, then either choose a different policy or policy set from the drop-down list, or add a new policy or policy set.
Step 5 Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.

Configuring Security Profiles

Editing a Security Profile for a Compute Firewall

Procedure

Step 1 Choose **Policy Management > Service Profiles > root > Compute Firewalls > Compute Security Profiles**.

Step 2 In the General tab, select the profile you want to edit, then click **Edit**.

Step 3 In the Edit Compute Security Profile dialog box, edit the fields as required by using the information in the following tables, then click **OK**.

Table 9: General Tab

Field	Description
Name	Profile name.
Description	Brief policy description.
Policy Set	List of available policy sets.
Add ACL Policy Set	Click to add a new ACL policy set.
Resolved Policy Set	Click the link to view and optionally edit the resolved policy set.
Resolved Policies	
(Un)assigned Policy	Click to assign or unassign policies.
Source Condition	Source condition for the policy.
Destination Condition	Destination condition for the policy.
Protocol	Protocol specify by the policy.
Ethertype	EtherType specified by the policy.
Action	Action to take if the specified condition is met.
Description	Brief policy description.

Table 10: Attributes Tab

Field	Description
Add User Defined Attribute	Click to add a custom attribute.
Name	Attribute name.
Value	Attribute value.

Editing a Security Profile for an Edge Firewall

This procedure enables you to edit a security profile associated with an edge firewall.

Procedure

Step 1 Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Security Profiles**.

Step 2 In the General tab, select the edge security profile that you want to edit, then click **Edit**.

Step 3 In the Edit Edge Security Profile dialog box, edit the entries as required by using the information in the following table, then click **OK**.

Field	Description
General Tab	
Name	Profile name.
Description	Brief profile description.
ID	Unique profile identifier.
Ingress Tab	
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Ingress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
Egress Tab	

Field	Description
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Egress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
NAT Tab	
Policy Set	Choose an existing policy set or click **Add NAT Policy Set** to add a new policy set. Click the **Resolved NAT Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
VPN Tab	
Policy Set	Choose an existing policy set or click **Add Interface Policy Set** to add a new policy set. Click the **Resolved VPN Interface Policy Set** link to modify the assigned policy set.
Advanced Tab	
Packet Inspection Policy	Choose an existing policy or click **Add Packet Inspection Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
Connection Timeout Policy	Choose an existing policy or click **Add Connection Timeout Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
Threat Migration	Choose an existing policy or click **Add TCP Intercept Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.

Field	Description
IP Audit Policy	Choose an existing policy or click **Add IP Audit Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.

Deleting a Security Profile

Procedure

Step 1 In the **Navigation** pane, choose **Policy Management** > **Security Policies**> **root** > **Security Profiles**.
Step 2 In the **Work** pane, click the security profile you want to delete.
Step 3 Click **Delete.**
Step 4 In the Confirm dialog box, click **OK**.

Deleting a Security Profile Attribute

Procedure

Step 1 In the **Navigation** pane, choose **Policy Management > Security Profiles > root > Security Profiles** > *security profile*. The security profile is the profile that contains the attribute you want to delete.
Step 2 In the **Work** pane, click the **Attributes** tab.
Step 3 Click the attribute you want to delete.
Step 4 Click **Delete.**
Step 5 In the Confirm dialog box, click **OK**.

Assigning a Policy

Procedure

Step 1 In the **Navigation** pane, expand **Policy Management** > **Security Profiles** > **root** > **Security Profiles**.
Step 2 Click the profile where you want to assign the policy.
Step 3 In the **Work** pane, click the **(Un)assign Policy** link.
Step 4 In the **(Un)assign Policy** dialog box, move the policy you want assigned to the **Assigned** list.
Step 5 Click **OK**.

Unassigning a Policy

Procedure

Step 1 In the **Navigation** pane, expand **Policy Management** > **Security Profiles** > **root** > **Security Profiles**.
Step 2 Click the profile where you want to unassign the policy.
Step 3 In the **Work** pane, click the **(Un)assign Policy** link.
Step 4 In the **(Un)assign Policy** dialog box, move the policy you want unassigned to the **Available** list.
Step 5 Click **OK**.

Configuring Security Policy Attributes

Configuring Object Groups

Adding an Object Group

Procedure

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Object Groups**.
Step 2 In the General tab, click **Add Object Group**.
Step 3 In the Add Object Group dialog box, complete the following fields, then click **OK**:

Note You must specify an attribute type and name before adding an object group expression. If VNMC was installed on Hyper-V hypervisor: the attribute type VM is not supported and if you choose the attribute type Network, attribute name Service is not supported.

Field	Description
Name	Object group name. This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description	Brief description of the object group. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Attribute Type	Available attribute types. You must configure an attribute type and name to add an object group expression.
Attribute Name	Available attribute names.
Expression Table	
Add Object Group Expression	Click to add an object group expression.
Operator	Operator for the selected expression.
Value	Value for the selected expression.

Adding an Object Group Expression

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group you want to add an object group expression to, then click **Edit**.

Note For new object groups, you must specify the attribute type and name before adding an object group expression.

Step 3 In the Edit Object Group dialog box, click **Add Object Group Expression**.

Step 4 In the Add Object Group Expression dialog box, specify the object group expression by using the information in the following table, then click **OK** in the open dialog boxes.

Field	Description
Attribute Name	Attribute (read-only).

Field	Description
Operator	Available operators for this attribute.
Attribute Value	Attribute value for this expression.

Editing an Object Group

Procedure

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group you want to edit, then click **Edit**.

Step 3 In the Edit Object Group dialog box, update the fields as follows, then click **OK** in the open dialog boxes:

Field	Description
Name	Object group name (read-only).
Description	Object group description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Attribute Type	Specified attribute type (read-only).
Attribute Name	Specified attribute name (read-only).
Expression Table	
Add Object Group Expression	Click to add a new object group expression.
Operator	Expression operator.
Value	Expression attribute value.

Editing an Object Group Expression

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group with the expression you want to edit, then click **Edit**.

Step 3 In the Expression table in the Edit Object Group dialog box, select the expression you want to edit, then click **Edit**.

Step 4 In the Edit Object Group Expression dialog box, edit the fields as required, then click **OK** in the open dialog boxes.

Field	Description
Attribute Name	Attribute name (read-only).
Operator	Available operators for this expression.
Attribute Value	Attribute value for this expression.

Deleting an Object Group

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the Object Group you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Deleting an Object Group Expression

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group that contains the expression you want to delete, then click **Edit**.

Step 3 In the Edit Object Group dialog box, select the expression that you want to delete In the Expression table, then click **Delete**.

Step 4 When prompted confirm the deletion.

Step 5 Click **OK** in the open dialog box to save the change.

Configuring Security Profile Dictionary

Adding a Security Profile Dictionary

Procedure

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Security Profile Dictionary**.

Note You can create one security profile dictionary at the root level and one for each tenant.

Step 2 In the General tab, click **Add Security Profile Dictionary**.

Step 3 In the Add Security Profile Dictionary dialog box, complete the following fields as appropriate, then click **OK**:

Field	Description
Name	Name of the security profile dictionary. This name can contain 1 to 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. **Note** You can create one security profile dictionary at the root level and one at the tenant level.
Description	A description of the security profile dictionary. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Attributes Table	

Field	Description
Add Security Profile Custom Attribute	Click to add a new attribute.
Name	Custom attribute name.
Description	Custom attribute description.

Adding a Security Profile Dictionary Attribute

Procedure

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary that you want to add an attribute to, then click **Edit**.

Step 3 In the Edit Security Profile Dictionary dialog box, click **Add Security Profile Custom Attribute**.

Step 4 In the Add Security Profile Custom Attribute dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Attribute name. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description	Attribute description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.

Editing a Security Profile Dictionary

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary you want to edit, then click **Edit**.

Step 3 In the Edit Security Profile Dictionary dialog box, modify the fields as appropriate, then click **OK**:

Field	Description
Name	Name of the security profile dictionary (read-only).
Description	Description of the security profile dictionary.
Attributes	
Add Security Profile Custom Attribute	Click to add a custom attribute.
Name	Attribute name.
Description	Attribute description.

Editing a Security Profile Dictionary Attribute

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary that contains the attribute you want to edit, then click **Edit**.

Step 3 In the Edit Security Profile Dictionary dialog box, select the attribute you want to edit, then click **Edit**.

Step 4 In the Edit Security Custom Attribute dialog box, edit the Description field as required, then click **OK** in the open dialog boxes to save the change.

Deleting a Security Profile Dictionary

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Deleting a Security Profile Dictionary Attribute

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**. In the General tab, select the dictionary that contains the attribute you want to delete, then click **Edit**.

Step 2 In the Edit Security Profile Dictionary dialog box, in Attributes table, select the attribute you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Working with vZones

A virtual zone (vZone) is a logical grouping of VMs or hosts. vZones facilitate working with policies and profiles because vZones enable you to write policies based on vZone attributes by using vZone names.

The high level flow for working with vZones in VNMC is as follows:

1. Define a vZone, each with one or more conditions for inclusion in the vZone.
2. Define a service policy with the rules based on zone or network conditions.
3. Create a policy set that includes the service policy defined in Step 2.
4. Create a security profile that includes the policy set created in Step 3.
5. Bind the security profile to the ASA 1000V or VSG port profile.
6. Assign the security profile to the ASA 1000V or VSG in VNMC.

See the following topics for more information about working with vZones.

Adding a vZone

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, click **Add vZone**.

Step 3 In the Add vZone dialog box provide the required information as described in the following table, then click **OK**:

Field	Description
Name	vZone name. The name can be between 2 and 32 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change the name after it is saved.
Description	vZone description. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Condition Match Criteria	Condition Match Options. • Choose match-all for the zone to match all the conditions (AND). • Choose match-any for the zone to match any one condition (OR). **Note** If VNMC is installed on Hyper-V Hypervisor, the Condition Match Criteria is disabled. The vZone must match all the conditions.
vZone Condition	
Attribute Type	Condition type. **Note** The VM and User Defined attribute types are not supported on Hyper-V Hypervisor.
Attribute Name	Condition attribute name. **Note** vZone conditions cannot be created using the service attribute.
Operator	Condition operator.
Attribute Value	Condition attribute value.

Editing a vZone

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, select the vZone that you want to edit, then click **Edit**.

Step 3 In the Edit vZone dialog box in the General tab, right-click the attribute that you want to edit, and choose **Edit**.

Step 4 In the Edit Zone Condition dialog box, edit the fields as required, then click **OK**in the open dialog boxes.

Field	Description
Name	vZone name (read-only).
Description	Brief vZone description.
Condition Match Criteria	Choose the required match option: • Match-all—Match all of the criteria (AND). • Match-any—Match any one of the criteria (OR). **Note** If VNMC is installed on Hyper-V Hypervisor, the Condition Match Criteria field is disabled. The vZone must match all conditions.
vZone Condition	
Attribute Type	Attribute type for the selected vZone condition (read-only).
Attribute Name	Attribute name for the selected vZone condition (read-only).
Operator	Operator for the selected vZone condition.
Attribute Value	Attribute value for the selected vZone condition.
Add Object Group **Note** Appears only when the member operator is selected.	Enables you to add an object group.

Deleting a vZone Condition

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, select the vZone with the condition that you want to delete, then click **Edit**.

Step 3 In the Edit vZone dialog box, select the condition in the vZone Condition table that you want to delete, then click **Delete**.

Step 4 Confirm the deletion.

Step 5 In the Edit vZone dialog box, click **OK** or **Apply**.

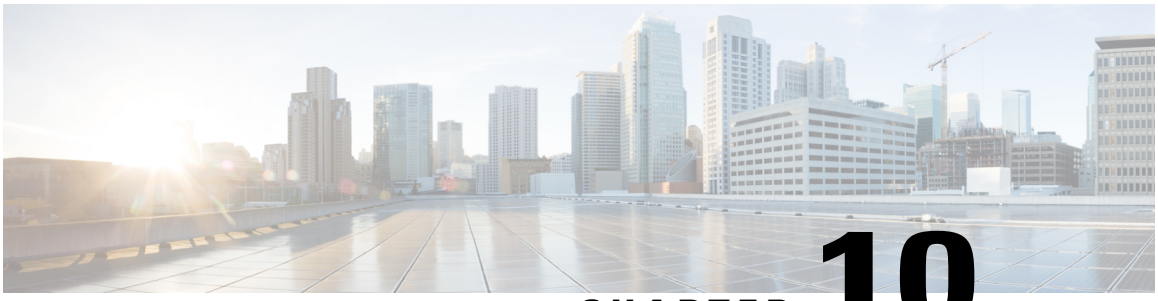
Deleting a vZone

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, select the vZones that you want to delete, then click **Delete**.

Step 3 Confirm the deletion.



CHAPTER 10

Configuring Device Policies and Profiles

This section includes the following topics:

- Device Policies and Profiles, page 137
- Device Configuration, page 138
- Device Policies, page 139
- Configuring Device Policies, page 139
- Configuring Device Profiles, page 165
- Configuring NTP, page 170
- Associating Device Policies with Profiles, page 172

Device Policies and Profiles

VNMC enables you to create device profiles and policies at any organizational level.

Device Profiles

A VNMC device profile is a set of custom security attributes and device policies. For Nexus 1000V VSMs, the device profile is added to the port profile. The port profile is assigned to the Nexus 1000V VSM vNIC, making the device profile part of the virtual machine (VM). Adding a device profile to the VM allows the addition of custom attributes to the VM. Firewall rules can be written using custom attributes such that traffic between VMs can be allowed to pass or be dropped.

You apply device profiles to compute and edge firewalls by choosing Resource Management > Managed Resources and then navigating to the required compute or edge firewall at the root or tenant level. The Firewall Settings area of the firewall pane includes the Device Profile option.

VNMC includes a default device profile at root level. The default device profile can be edited but cannot be deleted.

Policies

VNMC supports the following objects related to policies:

- Policy set—Contains policies. After a policy set is created, it can be assigned to a profile. An existing default policy set is automatically assigned at system boot up.
- Policy—Contains rules that can be ordered. An existing default policy is automatically assigned at system boot up. The default policy contains a rule with an action of **drop**.
- Rule—Contains conditions for regulating traffic. The default policy contains a rule with an action of **drop**. Conditions for a rule can be set using the network, custom, and virtual machine attributes.
- Object group—Can be created under an organization node. An object group defines a collection of condition expressions on a system-defined or user-defined attribute. An object group can be referred to in a policy rule condition when the member or not-member operator is selected. A rule condition that refers to an object group resolves to true if any of the expressions in the object group are true.
- Security Profile Dictionary—Logical collection of security attributes. You define dictionary attributes for use in a security profile. A security profile dictionary is created at the root or tenant node. You can create only one dictionary for a tenant and one for root. The security profile dictionary allows the user to define names of custom attributes. Custom attribute values are specified on security profile objects. Custom attributes can be used to define policy rule conditions. Attributes configured in a root level dictionary can be used by any tenant. You cannot create a dictionary below the tenant level.
- Zone—Set of VMs based on conditions. The zone name is used in the authoring rules.

Security policies are created and then pushed to the Cisco VSG or ASA 1000V.

Device Configuration

VNMC enables you to configure devices by adding policies to a device profile and then applying that profile to a device. Device profiles contain options for the following policies and settings:

- DNS server and domain
- NTP server
- SNMP policy
- Syslog policy
- Fault policy
- Core policy
- Log file policy
- Policy engine logging
- Authentication policy

Device Policies

VNMC enables you to create the following policies and assign them to device profiles for application to compute firewalls, edge firewalls, and VSGs:

- AAA policy
- Core file policy
- Fault policy
- Logging policy
- SNMP policy
- Syslog policy

VNMC provides default polices for fault, logging, SNMP, and syslog. The default policies cannot be deleted but can be modified. A device profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-Tenant Environment, on page 70.

Policies created under root are visible to both the VNMC profile and the Device profile.

Configuring Device Policies

VNMC enables you to configure and manage the following types of device policies:

- AAA
- Core file
- Fault
- Logging
- SNMP
- Logging

Configuring AAA Policies

AAA authentication policies verify users before they are allowed access to a network and network services. By creating AAA authentication policies in VNMC and associating the policies with objects through device profiles, you can ensure that only authenticated users can access the objects.

VNMC supports AAA authentication and authorization for edge firewalls, and server groups using the following protocols:

- Kerberos
- Lightweight Directory Access Protocol (LDAP)
- Windows NT
- RADIUS

- RSA SecurID (SDI)
- TACACS+

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > AAA > Auth Policies**.

Step 2 In the General tab, click **Add Auth Policy**.

Step 3 In the Add Auth Policy dialog box, enter the information as described in Add Auth Policy Dialog Box, on page 140, then click **OK**.

Note If you add a remote server group with a new server group with a new server host, the information that you must provide for the host depends on the protocol used. For example, the information required for a RADIUS server host is different from the information required for an LDAP server host.

See the online help for the information required for the selected protocol.

Field Descriptions

Add Auth Policy Dialog Box

Field	Description
Name	Policy name.
Description	Brief policy description.
Authorization	Check the Enable check box to enable authorization via server authentication.
Remote Access Methods	
Add Remote Access Method	Adds a remote access method to the policy. For more information, see Remote Access Method Dialog Box, on page 141.
Access Method	One of the following access methods: • Enable Mode • HTTP • Serial • SSH • Telnet

Field	Description
Admin State	Whether the administrative state of the policy is enabled or disabled.
Remote Server Group	Remote server group name.
Local Auth	This column is not used.

Remote Access Method Dialog Box

Field	Description
Access Method	One of the following access methods: • Enable Mode • HTTP • Serial • SSH • Telnet
Admin State	Whether the administrative state of the access method is enabled or disabled.
Server Group	Indicate the server group to use: **1** In the Protocol for Creation field, choose the required protocol. **2** In the Server Group fields, do one of the following: • From the drop-down list, choose an available remote server group. • Click **Add Remote Server Group - *protocol*** to add a new remote server group. **Note** If you add a new remote server group, the information that you must provide for the server group and host depends on the protocol used. For example, the information required for a RADIUS server group and host is different from the information required for an LDAP server group and host.

Configuring Core File Policies

Adding a Core File Policy for a Device

You can add a core file policy at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, click **Add Core File Policy**.

Step 3 In the Add Core File Policy dialog box, add the information as described in the following table, then click **OK**:

Field	Description
Name	Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved.
Description	Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.).
Admin State	Indicate whether the administrative state of the policy is to be enabled or disabled.
Hostname	Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in VNMC.
Port	Port number for sending the core dump file.
Protocol	Protocol for exporting the core dump file (read-only).
Path	Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/*test*, where *test* is the subfolder.

Editing a Core File Policy for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, select the core file policy you want to edit, then click **Edit**.

Step 3 In the Edit Core File Policy dialog box, edit the fields as required, using the information in the following table, then click **OK**.

Field	Description
Name	Name of the core file policy (read-only).
Description	Brief policy description.
Admin State	Administrative status of the policy: enabled or disabled.
Hostname	Hostname or IP address. **Note** If you use a hostname, you must configure a DNS server.
Port	Port number to use when exporting the core dump file.
Protocol	Protocol used to export the core dump file (read-only).
Path	Path to use when storing the core dump file on the remote system. The default path is /tftpboot. To specify a subfolder under tftpboot, use the format /tftpboot/*folder* where *folder* is the subfolder.

Deleting a Core File Policy from a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, select the core file policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring Fault Policies

Adding a Fault Policy for a Device Profile

You can add a fault policy at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, click **Add Fault Policy**.

Step 3 In the Add Fault Policy dialog box, enter the information as described in the following table, then click **OK**.

Field	Description
Name	Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief policy description.
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Action to be taken when faults are cleared: • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared.

Field	Description
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Editing a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, select the fault policy you want to edit, then click **Edit**.

Step 3 In the Edit Fault Policy dialog box, modify the following fields as required, then click **OK**.

Field	Description
Name	Policy name (read-only).
Description	Brief policy description.

Field	Description
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition recurs during the flapping interval, the fault returns to the active state. If the condition does not recur during the flapping interval, the fault is cleared. The next action depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Available fault retention actions: • retain—The system retains fault messages. • delete—The system deletes fault messages when they are marked as cleared.
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Deleting a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, select the fault policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring Log File Policies

Adding a Logging Policy for a Device Profile

You can add a logging policy for a device at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, click **Add Logging Policy**.

Step 3 In the Add Logging Policy dialog box, complete the following fields, then click **OK**.

Field	Description
Name	Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief policy description.

Field	Description
Log Level	One of the following logging severity levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Editing a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, select the log file policy that you want to edit, then click **Edit**.

Step 3 In the Edit Log File Policy dialog box, edit the fields as required by using the information in the following table, then click **OK**.

Field	Description
Name	Logging policy name (read-only).
Description	Brief policy description.
Log Level	One of the following logging levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Deleting a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, select the logging policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring SNMP Policies

Adding an SNMP Policy

You can add an SNMP policy at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, click **Add SNMP Policy**.

Step 3 In the Add SNMP dialog box, complete the following fields as appropriate:

Table 11: General Tab

Field	Description
Name	SNMP policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	SNMP policy description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Admin State	Indicate whether the administrative status of the policy is enabled or disabled.
Location	Physical location of the device.
Contact	Contact person for the device.
SNMP Port	Port that the SNMP agent listens to for requests. You cannot edit this field.

Step 4 Click the **Communities** tab, then complete the following steps:

a) Click **Add SNMP Community**.

b) In the Add SNMP Community dialog box, complete the following fields as appropriate, then click **OK**:

Name	Description
Community	SNMP community name.
Role	Role associated with the community string. You cannot edit this field.

Step 5 In the Add SNMP dialog box, click **OK**.

Editing an SNMP Policy

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy that you want to edit, then click **Edit**.

Step 3 In the Edit SNMP Policy dialog box, edit the information in the General tab as required, using the information in the following table:

Field	Description
Name	SNMP policy name (read-only).
Description	Brief policy description.
Admin State	Administrative state of the policy: enabled (default) or disabled.
Location	Physical location of the device.
Contact	Contact person for the device.
SNMP Port	Port that the SNMP agent listens to for requests (read-only).

Step 4 In the Communities tab, edit the information as required:

Field	Description
Add SNMP Community	Click to add an SNMP community.
Community	SNMP community name.
Role	Role associated with the SNMP community.

Step 5 In the Traps tab, edit the information as required:

Field	Description
Add SNMP Trap	Click to add an SNMP trap.
Hostname	IP address of the SNMP host.
Port	Port where the SNMP agents listens for requests.
Community	SNMP community name.

Step 6 Click **OK**.

Deleting an SNMP Policy

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding an SNMP Trap Receiver

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, click **Add SNMP Policy > Traps > Add SNMP Trap.**.

Step 3 In the Add SNMP Trap dialog box, enter the following information, then click **OK**:

Field	Description
Hostname/ IP Address	Hostname or IP address of the SNMP host.
Port	Port that the SNMP agent listens to for requests. The default port is 162.
Community	SNMP community name.

Editing an SNMP Trap Receiver

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy with the SNMP trap that you want to edit, then click **Edit**.

Step 3 In the Edit SNMP Policy dialog box, click the **Traps** tab.

Step 4 In the Traps tab, select the entry that you want to edit, then click **Edit**.

Step 5 In the Edit SNMP Trap dialog box, edit the information in the General tab as required, using the following information:

Field	Description
Hostname/IP Address	Hostname or IP address of the SNMP host (read-only).
Port	Port that the SNMP agent listens to for requests.
Community	SNMP community name.

Step 6 Click **OK** in the open dialog boxes.

Deleting an SNMP Trap Receiver

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
Step 2 In the General tab, select the SNMP policy with the SNMP trap that you want to delete, then click **Edit**.
Step 3 In the Edit SNMP Policy dialog box, click the **Traps** tab.
Step 4 In the Traps tab, select the entry that you want to delete, then click **Delete**.
Step 5 When prompted, confirm the deletion.

Configuring Syslog Policies

Adding a Syslog Policy for a Device

VNMC enables you to configure syslog policies for syslog messages and then attach a created syslog policy to a device profile for implementation on all devices using that profile.

You can create syslog policies for logging syslog messages to a remote syslog server or to a local buffer for later review.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
Step 2 In the General tab, click **Add Syslog Policy**.
Step 3 In the Add Syslog dialog box, provide the information as described in Add Syslog Policy Dialog Box, on page 154, then click **OK**.

Field Descriptions

Add Syslog Policy Dialog Box

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.

Field	Description
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
Monitor area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.

Field	Description
File area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.

Editing a Syslog Policy for a Device Profile

VNMC enables you to edit existing syslog policies as described in this procedure.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the policy you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, in the General tab, edit the information as required, using the following information:

Field	Description
Name	Policy name (read-only).

Field	Description
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs.

Step 4 In the Servers tab, click **Add Syslog Server** to add a new syslog server, or select an existing server and click **Edit** to edit it.

Step 5 In the Local Destinations tab, edit the information as required, using the following information:

Field	Description
Console area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.
Monitor area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Field	Description
File area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.
Buffer area	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory with the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.

Step 6 Click **OK**.

Deleting a Syslog Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the syslog policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding a Syslog Server for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, click **Add Syslog Policy**.

Step 3 In the Add Syslog Policy dialog box, click the **Servers** tab, then click **Add Syslog Server**.

Step 4 In the Add Syslog Server dialog box, provide the information as described in Add Syslog Server Dialog Box, on page 160, then click **OK** in the open dialog boxes.

Field Descriptions

Add Syslog Server Dialog Box

Field	Description
Server Type	One of the following server types: • primary • secondary • tertiary

Field	Description
Hostname/IP Address	Hostname or IP address where the syslog file resides. **Note** If you use a hostname, you must configure a DNS server.
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)

Field	Description
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	Administrative state of the server: enabled or disabled.
Port	Port to use to send data to the syslog server. The default port selection is 514 for UDP.
Protocol	Protocol to use: TCP or UDP (default).
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.
Server Interface	Interface to use to access the syslog server.

Editing a Syslog Server for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the required syslog policy, then choose **Edit**.

Step 3 In the Edit Syslog Policy dialog box, from the **Servers** tab, select the syslog server you want to edit, then click **Edit**

Step 4 In the Edit Syslog Server dialog box, edit the fields as required, using the information in the following table.

Field	Description
Server Type	One of the following server types: primary, secondary, or tertiary (read-only).
Hostname/IP Address	Hostname or IP address where the syslog file resides.
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)

Field	Description
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	Administrative state of the policy: enabled or disabled.
Port	Port to use to send data to the syslog server. Valid port values are 1025 through 65535 for both TCP and UDP. The default TCP port is 1470. The default UDP port is 514.
Protocol	Protocol to use: TCP or UDP.
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.

Field	Description
Server Interface	Interface to use to access the syslog server. This option applies to ASA 1000V only. Enter the data interface name specify in the edge firewall. Use the device CLI to configure a route through the management interface.

Step 5 Click **OK** in the open dialog boxes to save your changes.

Deleting a Syslog Server for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
Step 2 In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.
Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.
Step 4 In the Servers tab, select the syslog server that you want to delete, then click **Delete**.
Step 5 When prompted, confirm the deletion.
Step 6 Click **OK** to save the policy.

Configuring Device Profiles

Adding a Firewall Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.
Step 2 In the General tab, click **Add Device Profile**.
Step 3 In the New Device Profile dialog box, enter the required information in the General and Policies tabs, then click **OK**:

Field	Description
General Tab	

Field	Description
Name	Device profile name. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description	Brief profile description.
Time Zone	Choose the required time zone from the drop-down list.
Policies Tab	
DNS Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.
DNS Domains	You can: • Add a new domain. • Select an existing domain and edit or delete it.
NTP Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.
SNMP	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Syslog	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.

Field	Description
Fault	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Core File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Policy Agent Log File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Policy Engine Logging	Select the appropriate radio button to enable or disable logging.
Auth Policy	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.

Editing a Firewall Device Profile

After you create a firewall device profile, you can edit it as needed.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.

Step 2 In the Device Profiles pane, select the profile you want to edit, then click **Edit**.

Step 3 In the Edit Firewall Device Policy dialog box, update the information in the General tab as described in the following table:

Field	Description
Name	Profile name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief profile description. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon.
Time Zone	Select the required time zone from the drop-down list.

Step 4 In the Policies tab, update the information as described in the following table:

Field	Description
DNS Servers	
Add DNS Server	Click to add a DNS server.
Delete	Click to deletes the DNS server IP address selected in the IP Address table.
Up and down arrows	Change the priority of the selected NTP Server hostname.
IP Address table	IP addresses for the DNS servers configured in the system. VNMC uses the DNS servers in the order they appear in the table.
NTP Servers	
Add NTP Server	Click to add an NTP server.
Delete	Click to delete the NTP server hostname selected in the Hostname table.

Field	Description
Up and down arrows	Change the priority of the selected NTP Server hostname.
IP Address table	Contains the NTP server hostnames configured in the system. VNMC uses the NTP server hostnames in the order they appear in the table.
DNS Domains	
Add	Click to add a DNS domain name.
Edit	Click to edit the DNS domain name selected in the DNS Domains table. The default DNS name cannot be edited.
Delete	Click to delete the DNS domain name selected in the DNS Domains table.
DNS Domains table	Default DNS domain name and domain in the system.
Other Options	
SNMP	Select, add, or edit SNMP policies as needed.
Syslog	Select, add, or edit syslog policies as needed.
Fault	Select, add, or edit fault policies as needed.
Core File	Select, add, or edit core file policies as needed.
Policy Agent Log File	Select, add, or edit the policy agent log file policies as needed.
Policy Engine Logging	Select the appropriate radio button to enable or disable logging.
Auth Policy	Select an available authentication policy, or click **Add Auth Policy** to add a new authentication policy.

Step 5 Click **OK**.

Deleting a Firewall Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root** > **Device Profiles**.

Step 2 In the **Work** pane, click the device profile you want to delete.

Step 3 Click **Delete.**

Step 4 In the Confirm dialog box, click **OK**.

Configuring NTP

Network Time Protocol (NTP) is a networking protocol used to synchronize the time on a network of machines. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server.

VNMC enables you to configure NTP for compute firewalls, edge firewalls, and VNMC itself.

Configuring NTP for a compute or edge firewall requires the following steps:

1 Configuring a device profile with NTP.

2 Applying the device profile to a compute or edge firewall

The following topics describe how to perform these steps.

For information on configuring NTP on VNMC, see Adding an NTP Server, on page 59.

Creating a Device Profile with NTP

This procedure describes how to create a device profile with NTP that you can apply to an edge or compute firewall.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.

Step 2 In the General tab, click **Add Device Profile**.

Step 3 In the New Device Profile dialog box, provide the following information:

- Name—Profile name.
- Description—Brief profile description.
- Time Zone—From the drop-down list, choose the time zone.

Step 4 Click the **Policies** tab.

Step 5 In the NTP servers area, click **Add NTP Server**.

Step 6 In the Add NTP Server dialog box, enter the information as described in Add NTP Server Dialog Box, on page 171, then click **OK**.

Step 7 Click **OK**.

What to Do Next

After you have configured the device profile, you can apply it to a firewall as described in the following topics:

- Applying Device Profiles to Edge Firewalls, on page 172
- Applying Device Profiles to Compute Firewalls, on page 172

Field Descriptions

Add NTP Server Dialog Box

Field	Description
Hostname/IP Address	NTP server name or IP address. For VNMC and VSGs, you can enter either a hostname or IP address. For ASA 1000Vs, you must enter an IP address.

Interface Name	Device interface to reach the NTP server.
	The following information applies:
	• Only ASA 1000Vs support interface names:
	  • If you specify an interface, use the interface name specified by the edge firewall.
	  • To use the management interface, you must configure the route by using the CLI.
	• VSGs do not support interface names.
	• This field is not displayed for VNMC NTP server configuration.

Field	Description
Authentication Key	Authentication key to access the NTP server. The following information applies: • Only ASA 1000Vs support authentication keys. • VSGs do not support authentication keys. • This field is not displayed for VNMC NTP server configuration.

Applying Device Profiles to Compute Firewalls

After you have created a device profile, you can apply the profile to a compute firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.

Step 2 In the General tab, click **Select** in the Device Profile field.

Step 3 In the Select Device Profile dialog box, select the desired profile, then click **OK**.

Step 4 Click **Save**.

Applying Device Profiles to Edge Firewalls

After you have created a device profile, you can apply the profile to an edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.

Step 2 In the General tab, click **Select** in the Device Profile field.

Step 3 In the Select Device Profile dialog box, select the desired profile, then click **OK**.

Step 4 Click **Save**.

Associating Device Policies with Profiles

After you create a device policy, you can associate it with a device profile. By doing so, you can ensure that all devices associated with the device profile use the same policy.

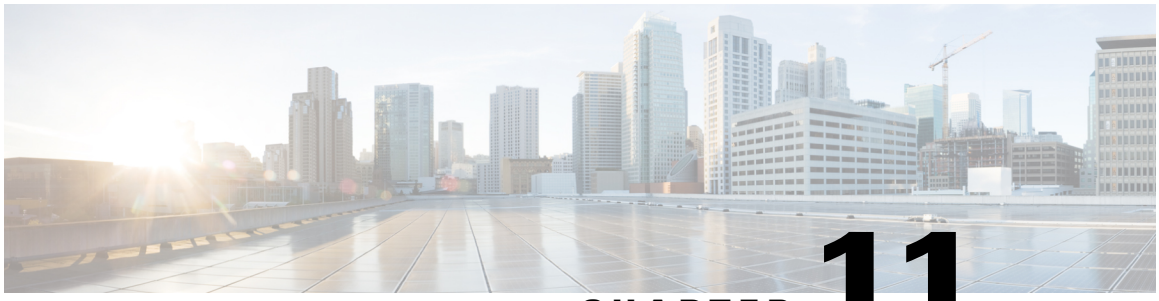
Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles >** *profile* where *profile* is the device profile that you want to add the device policy to.

Step 2 Click the **Policies** tab.

Step 3 In the Policies tab, locate the drop-down list for the type of policy you want to associate, such as Syslog or Auth Policy.

Step 4 From the drop-down list, choose the policy to add to the profile, then click **Save**.
The policy is automatically applied to all devices using the selected profile.



CHAPTER 11

Configuring Managed Resources

This section includes the following topics:

- Resource Management, page 175
- Resource Manager, page 176
- Virtual Machines, page 176
- Virtual Security Gateways, page 176
- ASA 1000V Cloud Firewalls, page 177
- Managing Compute Firewalls, page 177
- Managing Edge Firewalls, page 182
- Verifying VM Registration in VNMC, page 185
- Examining Fault Details, page 185
- Launching ASDM from VNMC, page 187
- Managing Pools, page 190

Resource Management

The Resource Management tab displays the following resources that are managed by VNMC:

- Virtual Machines (VMs)
- ASA 1000V edge firewalls
- VSG compute firewalls
- Virtual Supervisor Modules (Nexus 1000V VSM)

You manage ASA 1000Vs and VSGs by placing them in service:

- You place an ASA 1000V in service by creating an edge firewall in an organization and assigning the ASA 1000V to that edge firewall.

- You place a VSG in service by creating a compute firewall in an organization and assigning the VSG to that compute firewall.

You manage VMs by discovering those VMs that have at least one network interface configured with a Nexus 1000V port profile.

Resource Manager

Resource Manager manages logical edge and compute firewalls and their association with ASA 1000Vs and VSGs, respectively. When an edge firewall is associated with an ASA 1000V, the device configuration profile information (defined by the edge firewall) is pushed to the ASA 1000V which, in turn, triggers the ASA 1000V to download the security profiles and policies from Policy Manager.

Resource Manager is responsible for the following services:

- Maintaining an inventory of ASA 1000Vs, VSGs, and VSMs.
- With user input, defining compute firewalls and associating them with VSGs for provisioning.
- With user input, defining edge firewalls and associating them with ASA 1000Vs for provisioning.
- Integrating with VMware vCenter instances to retrieve VM attributes.

Virtual Machines

Virtualization allows you to create multiple VMs that run in isolation, side by side on the same physical machine. Each VM has virtual RAM, a virtual CPU and NIC, and an operating system and applications. Because of virtualization, the operating system sees a consistent set of hardware regardless of the actual physical hardware components.

VMs are encapsulated in files for rapid saving, copying, and provisioning, which means that you can move full systems, configured applications, operating systems, BIOS, and virtual hardware within seconds, from one physical server to another. Encapsulated files allow for zero-downtime maintenance and continuous workload consolidation.

Instances of VNMC are installed on VMs.

Virtual Security Gateways

VSGs evaluate VNMC policies based on network traffic. The main functions of a VSG are as follows:

- Receive traffic from Virtual Network Service Data Path (vPath).

  For every new flow, the vPath component encapsulates the first packet and sends it to a VSG as specified in the Nexus 1000V port profiles. It assumes that the VSG is Layer 2 adjacent to vPath. The mechanism used for communication between vPath and the VSG is similar to VEM and Nexus 1000V VSM communication on a packet VLAN.
- Perform application fix-up processing such as FTP, TFTP, and RSH.
- Evaluate policies by inspecting the packets sent by vPath using network, VM, and custom attributes.
- Transmit the policy evaluation results to vPath.

Each vPath component maintains a flow table for caching VSG policy evaluation results.

ASA 1000V Cloud Firewalls

The Cisco Adaptive Security Appliance 1000V Cloud Firewall (ASA 1000V) is a virtual appliance that was developed using the ASA infrastructure to secure the tenant edge in multi-tenant environments with Cisco Nexus 1000V deployments. ASA 1000V firewalls provide the following edge features and functionality:

- Supports site-to-site VPN, NAT, and DHCP.
- Acts as a default gateway.
- Secures the VMs within a tenant against any network-based attacks.

In VNMC, edge firewall objects are associated to an ASA 1000V instance. After association, all applicable profile types for the ASA 1000V device type are pushed to the ASA 1000V instance. All edge profile objects that are created at the same organization level as the edge firewall object are pushed to the device.

Managing Compute Firewalls

VNMC enables you to add, edit, and delete compute firewalls. In addition, you can assign a VSG to compute firewall, thereby placing the VSG in service. The following topics describe these activities in more detail.

Adding a Compute Firewall

This procedure describes how to add a compute firewall to VNMC so that you can assign it to a VSG, and thereby place the VSG in service.

When you add a new compute firewall, the firewall data IP address can be the same as the data IP address of an existing compute firewall in VNMC as long as the firewalls have different organizational paths. That is, as long as the firewalls do not reside in the same organization, including parent and child organizations.

Note We recommend that you add the compute firewall at the tenant level or below, and not at the root level.

Procedure

Step 1 In the Resource Management tab, choose **Managed Resources > root >** *tenant* **> Compute Firewalls**.

Step 2 In the General tab, click **Add Compute Firewall**.

Step 3 In the Add Compute Firewall dialog box, supply the required information as described in the following table, then click **OK**:

Field	Description
Name	Object name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief object description.
Firewall Settings Area	
Device Profile	To apply a device profile to the firewall: **1** Click **Select**. **2** In the Select Device Profile dialog box, choose the required profile, then click **OK**.
Management Hostname	Management hostname for the firewall.
Data IP Address	Data IP address. The vPath component running on each VEM uses the data IP address to determine the MAC address of the VSG (via ARP). After the VSG MAC address has been resolved, vPath can communicate with the VSG using MAC in MAC encapsulation. Subsequently, for each new flow initiated by a VM, vPath sends the first packet of the flow to the VSG for policy evaluation. vPath caches the VSG policy decision in a flow table. This is the same IP address that is configured in the **vservice** CLI command on the Nexus 1000V port profile.
Data IP Subnet	Data IP subnet.

Editing a Compute Firewall

You can edit existing compute firewalls as needed.

Procedure

Step 1 In the Resource Management tab, choose **Managed Resources > root >** *tenant* **> Compute Firewalls >** where *tenant* is the required tenant.

Step 2 In the General tab, select the compute firewall you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, modify the following fields as appropriate, using the information in the following tables, then click **OK**.

General Tab

Field	Description
Name	Compute firewall name (read-only).
Description	Brief firewall description.
Pool Name	The pool assigned to the compute firewall, if any. Only one pool can be assigned to a compute firewall at a time. To change the pool, click **Assign Pool**.
States	
Config State	One of the following compute firewall configuration states: not-applied, applying, failed-to-apply, or applied.
Association State	One of the following compute firewall association states: unassociated, associating, associated, disassociating, or failed.
Faults Associated with Firewall	Displays faults associated with the firewall. This information is available only if the compute firewall has been associated with a VSG.
View Device Faults	Displays faults associated with the device. This information is available only if the compute firewall has been associated with a VSG.
Firewall Settings	
Device Profile	Device profile associated with the firewall. To change the device profile, click **Select**, then choose the desired profile.

Field	Description
Management Hostname	Management hostname for the compute firewall.
Data IP Address	Compute firewall data IP address. The vPath component running on each VEM uses the data IP address to determine the MAC address of the VSG (via ARP). Once the VSG MAC address has been resolved, vPath can communicate with the VSG using MAC in MAC encapsulation. Subsequently for each new flow initiated by a VM, vPath sends the first packet of the flow to the VSG for policy evaluation. vPath caches the VSG policy decision in a flow table. This is the same IP address which is configured in the **vservice** CLI command on the Nexus 1000v port profile.
Data IP Subnet	Firewall data IP subnet mask.
VSG Details This information is available only if the compute firewall has been associated with a VSG.	
Task	Click to open the Edit VSG dialog box.
VSG Service ID	Internal identification number of the VSG.
VSG Mgmt IP	VSG management IP address.
HA Role	High availability (HA) role of the VSG: HA or standalone mode.
Association	Association state of the VSG: unassociated, associating, associated, disassociating, or failed.
Reachable	Whether or not the VSG can be reached.

Compute Security Profiles Tab

Field	Description
Show Resolved Policies	Click to view and optionally modify the security policies applied to the compute firewall. This option is available only if the selected profile has been configured in the corresponding VSM port profile.
Properties	Displays the properties of the port profile associated with the compute firewall.

Field	Description
Compute Security Profile	Name of the compute firewall security profile.
Port Profile	Name of the associated port profile.
Org	Distinguished name (DN) of the organization.
VSG Data IP	VSG data IP address.
Config State	VSG configuration state.

Deleting a Compute Firewall

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls**.

Step 2 In the General tab, select the compute firewall you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Assigning a VSG

Assigning a VSG to a compute firewall enables you to place a VSG in service and manage it using VNMC. Before you can assign a VSG to a compute firewall, you must:

- Register the VSG with VNMC. For information on registering a VSG with VNMC, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide*.
- Add a compute firewall toVNMC. For more information, see Adding a Compute Firewall, on page 177.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls**.

Step 2 In the General tab, select the compute firewall to which you want to assign a VSG, then click **Assign VSG**.

Step 3 In the Assign VSG dialog box, select the desired IP address from the **VSG Management IP** drop-down list, then click **OK**.

Unassigning a VSG

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls**.

Step 2 In the Compute Firewalls table, select the firewall with the VSG you want to unassign.

Step 3 Click **Unassign VSG/Pool**.

Step 4 In the Confirm dialog box, click **Yes**.

Managing Edge Firewalls

Managing edge firewalls involves adding edge firewalls to VNMC, configuring the edge firewall data interfaces, and then assigning an ASA 1000V to the edge firewall to place the ASA 1000V in service. The following topics describe these activities in more detail.

Adding an Edge Firewall

This procedure describes how to add an edge firewall to VNMC so that you can assign it to an ASA 1000V instance, and thereby place the ASA 1000V in service.

When you add a new edge firewall, the firewall data IP address identified as the primary IP address of the inside data interface can be the same as the IP address of an inside data interface for an existing edge firewall in VNMC long as the firewalls have different organizational paths. That is, as long as the edge firewalls do not reside in the same organization, including parent and child organizations.

Note We recommend that you add edge firewalls at the tenant level or lower, and not at the root level.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls**.

Step 2 Click **Add Edge Firewall**.

Step 3 In the Add Edge Firewall dialog box, specify the information as described in Add Edge Firewall Dialog Box, on page 183, then click **OK**.

What to Do Next

After you add the edge firewall, assign an ASA 1000V to it so that you can manage the ASA 1000V using VNMC. For more information, see Assigning an ASA 1000V, on page 184.

Add Edge Firewall Dialog Box

Field	Description
Name	Edge firewall name.
Description	Brief description of the edge firewall.
HA Mode	High Availability (HA) role of the edge firewall: HA or standalone.
Device Profile	To apply a device profile: **1** Click **Select**. **2** In the Select Device Profile dialog box, choose the desired profile and click **OK**.
Edge Device Profile	To apply an edge device profile: **1** Click **Select**. **2** In the Select Edge Device Profile dialog box, choose the desired profile, then click **OK**.

Adding a Data Interface

When you add an edge firewall, you also need to specify inside and outside interfaces for data communications.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls**.

Step 2 In the Edge Firewalls pane, select the edge firewall to add or modify data interfaces, then click **Edit**.

Step 3 In the Edit Edge Firewall dialog box, click **Add Data Interface**.

Step 4 For each interface you add, enter the information as described in Add Data Interface Dialog Box, then click **OK**.

Add Data Interface Dialog Box

Field	Description
Name	Interface name.
Description	Brief interface description.

Field	Description
Role	Whether the interface is for inside or outside communications.
DHCP	Available for outside interfaces only. Check the **Enable DHCP** check box to enable DHCP on the interface.
Primary IP Address	IP address for this interface.
Secondary IP Address	Available if the edge firewall is in High Availability (HA) Mode. Secondary IP address for this interface.
Subnet Mask	Mask to apply to the IP address.
Edge Security Profile	Available for outside interfaces only. To apply an edge security profile: 1 Click **Select**. 2 In the Select Edge Security Profile dialog box, choose the desired profile, then click **OK**.

Assigning an ASA 1000V

After you add an edge firewall to VNMC, you need to assign an ASA 1000V instance to it so that the ASA 1000V instance is placed in service with the associated policies and profiles. Before you can assign an ASA 1000V to an edge firewall, you must:

- Register the ASA 1000V to VNMC. For more information, see the *Cisco Virtual Network Management Center 2.0 Quick Start Guide*.
- Add an edge firewall to VNMC. For more information, see Adding an Edge Firewall, on page 182.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.

Step 2 Click **Assign ASA 1000V**.

Step 3 In the Assign ASA 1000V dialog box, choose the required ASA 1000V from the drop-down list, then click **OK**.

Unassigning an ASA 1000V

If required you can unassign an ASA 1000V from an edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.

Step 2 Click **Unassign ASA 1000V/Pool**.

Step 3 In the confirmation dialog box, click **OK**.

Verifying VM Registration in VNMC

Use this procedure to verify that the following VMs are successfully registered in VNMC:

- ASA 1000V
- Cloud VSM
- VSG
- VSM

Procedure

Step 1 Choose **Administration > Service Registry > Clients**.

Step 2 In the Clients table, confirm that the Open State column contains *registered* for the ASA 1000V, VSG, VSM, and cloud VSM entries.

Examining Fault Details

VNMC enables you to examine the policy and configuration errors that prevent the successful application of a policy. For example, if you apply a policy to an edge firewall and the Config State field displays the Failed-to-Apply state, you can examine the configuration errors to identify the issue and resolve the problem.

The same interface enables you to perform the following tasks:

- Examine the faults and events associated with an edge firewall with applied policies and configurations.
- Examine the faults associated with a compute firewall.

The following topics describe these features in more detail.

Examining Faults and Configuration Errors for Edge Firewalls

VNMC enables you to view the faults and events associated with edge firewalls, and their policies and configurations.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.

Step 2 In the General tab, review the configuration, association, and fault information in the States area.

Step 3 If faults are indicated, view fault details as follows:

- Click the **Faults** tab.
- Click the **Events** tab.
- Click **Faults Associated with Firewall**.
- Click **View Configuration Faults**.

Step 4 To view more information, double-click an entry in any of the tables.
In the Faults table in the new browser window, you can click **Refresh Now** to view updated information.

Examining Faults for Compute Firewalls

VNMC enables you to examine faults and events for compute firewalls.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.

Step 2 In the General tab, review the configuration, association, and fault information in the States area.

Step 3 If faults are indicated, view fault details as follows:

- Click the **Faults** tab.
- Click the **Events** tab.
- Click **Faults Associated with Firewall**.
- Click **View Configuration Faults**.

Step 4 To view more information, double-click an entry in any of the tables.

Launching ASDM from VNMC

VNMC enables you to launch Cisco Adaptive Security Device Manager (ASDM) as a Web Start application on your desktop.

You can set up ASDM to be used by the ASA 1000V when it is configured for either VNMC management mode or ASDM management mode. When the ASA 1000V is configured to use VNMC management mode, you can use ASDM to monitor the status of the ASA 1000V, but you cannot use it to manage configurations.

Before You Begin

You must complete the following tasks before launching ASDM from VNMC:

1. Do one of the following:
   - If you have not already deployed the ASA 1000V OVA, do so now; during the deployment, provide the ASDM client IP address.
   - If you have already deployed the ASA 1000V OVA, apply the following configuration by using the VM console in the vSphere client:
     - Add a route on the management interface to the ASDM client subnet by issuing the following command:
       ```
       ASA1000V(config)# route interface ip subnet next-hop-ip
       ```
       where *interface* is the management interface to the ASDM client subnet, *ip* is the IP address of the host that accesses ASDM, *subnet* is the ASDM client subnet, and *next-hop-ip* is the IP address of the gateway.

       Note Perform this step only if the next hop gateway IP address was not specified when deploying the ASA 1000V.

     - Allow HTTP access via the management interface for the ASDM client subnet by entering the following command:
       ```
       ASA1000V(config)# http ip subnet interface
       ```
       where *ip* is the IP address of the host that accesses ASDM, and *interface* is the ASDM client interface.

       Note Perform this step only if the ASDM client IP address was not specified when deploying the ASA 1000V.

2. Confirm the following:
   - The ASA 1000V is registered to VNMC.
   - A valid username and password exist for the ASA 1000V VM console.
3. Assign the edge firewall to an ASA 1000V instance. If the edge firewall is not assigned to an ASA 1000V instance, the ASDM options are not displayed in the UI.
4. Confirm that your system is configured to run downloaded Java Web Start applications.

For more information about configuring ASDM, see the *Cisco ASA 1000V Cloud Firewall Getting Started Guide*.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall* where *edge-firewall* is the edge firewall for which you want to launch ASDM.

Step 2 In the General tab, click **Launch ASDM** in the ASA 1000V Details area. See Example Screens for ASDM, on page 189.
The ASDM Launch screen opens in a new browser window.

Step 3 In the ASDM Launch screen, click **Run ASDM**.
The ASDM Web Start application is automatically downloaded and runs. If prompted, accept the certificates.
Note If an ASDM login dialog box is displayed, you can click **OK** without entering login credentials.

ASDM opens in a new window on your desktop as shown in Example Screens for ASDM, on page 189.

Example Screens for ASDM

Figure 4: Launch ASDM Link in the VNMC Interface

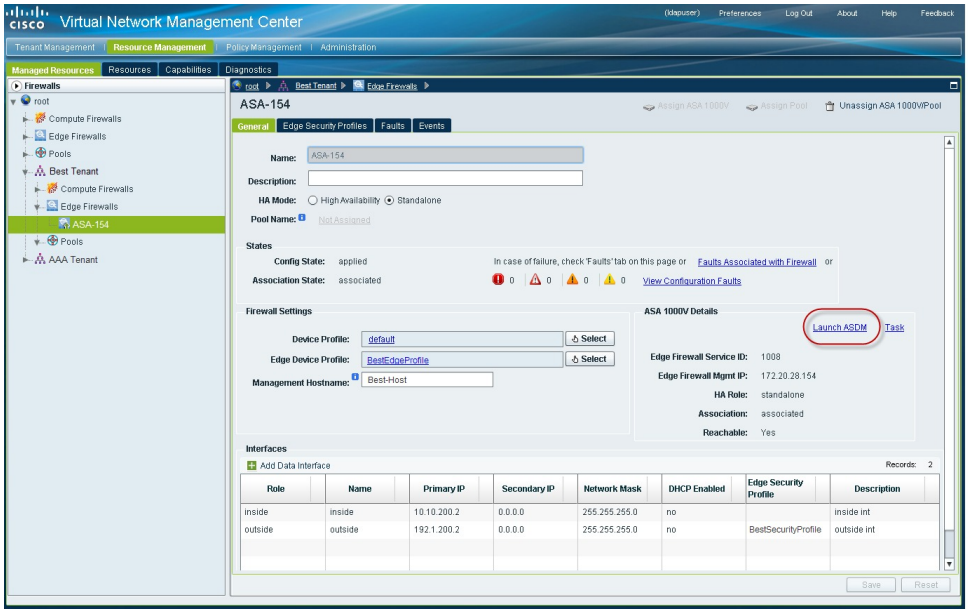
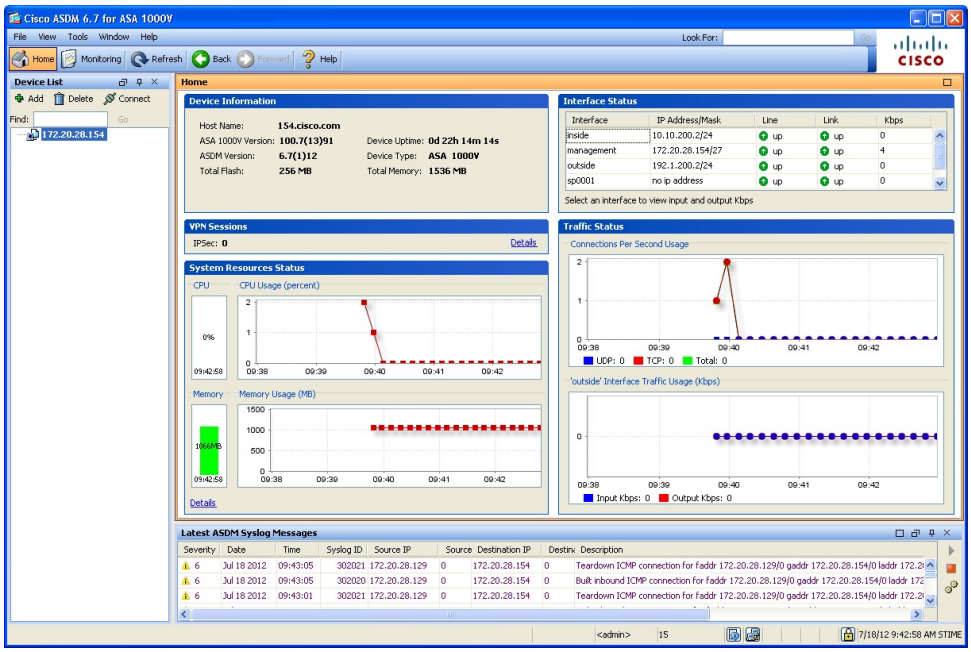


Figure 5: ASDM Window



Managing Pools

Adding a Pool

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Pools**.

Step 2 In the General tab, click **Add Pool**.

Step 3 In the Add Pool dialog box, enter the information as described in the following table, then click **OK**:

Field	Description
Name	Pool name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief pool description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Pool Members Area	
(Un)Assign	Click to add pool members to or remove pool members from the pool.
Management IP Address	Management IP address of the pool member.
Firewall	Associated compute or edge firewall.
Association State	Association state of the pool member: unassociated, associating, associated, disassociating, or failed.
Service ID	Unique identifier for the pool member.
Operational State	Pool member operational state.

Step 4 (Optional) Assign pool members to the pool by performing the following tasks:

a) Click **(Un)Assign**.

b) In the (Un)Assign Pool Member(s) dialog box, select the firewall that you want to assign, and then click the arrow to move it to the Assigned Firewalls list.

c) Click **OK**.

Step 5 Click **OK**.

Assigning a Pool

After you have created a pool, you can assign it to a compute or edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root > Compute Firewalls** or **Edge Firewalls**.

Step 2 In the list of firewalls, select the required firewall, then click **Assign Pool**.

Step 3 In the Assign Pool dialog box, either choose a pool from the Name drop-down list or click **Add Pool** to add a new pool.

Step 4 Click **OK**.

Editing a Pool

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Pools**.

Step 2 In the General tab, select the pool that you want to edit, then click **Edit**.

Step 3 In the Edit Pool dialog box, edit the information as required by using the information in the following table, then click **OK**.

Field	Description
Name	Pool name (read-only).
Description	Brief pool description.
Pool Members	
(Un)Assign	Click to assign or unassign pool members.
IP Address	Pool member IP addresses.
Compute Firewall	A list of the compute firewalls.
Association State	Association state for the pool member.
Service ID	Service identification number for the pool member.

Field	Description
Operational State	Operational state of the pool member.

Unassigning a Pool

If required, you can unassign a pool from a compute or edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root > Compute Firewalls** or **Edge Firewalls**.

Step 2 In the list of firewalls, select the required firewall, then click **Unassign** *object*/**Pool** where *object* is either ASA 1000V or VSG, depending on whether you selected an edge or compute firewall.

Step 3 When prompted, confirm the deletion.

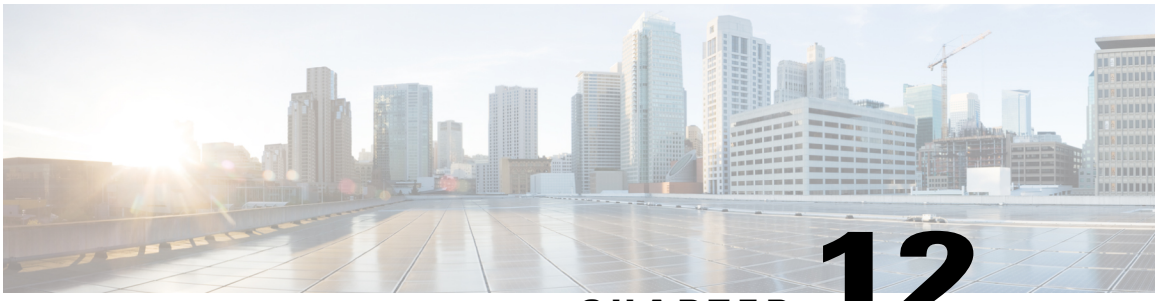
Deleting a Pool

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Pools**.

Step 2 In the General tab, select the pool you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.



CHAPTER 12

Configuring Administrative Operations

This section includes the following topics:

- Administrative Operation Conventions, page 193
- Managing Backup Operations, page 193
- Restoring a Backup Configuration, page 198
- Managing Export Operations, page 200
- Configuring Import Operations, page 204

Administrative Operation Conventions

The following conventions apply when performing the administrative operations described in this section:

- The remote file location you specify must start with a slash (/) and include the full path and file name. Do not use relative paths.
- The user name and password on the remote system must be correct, and the user specified must have read and write permissions on the remote system.
- The file on the remote system must be a valid file, and the size cannot be zero.
- For backup and export operations, if the Task tab contains a Remote Err Description of *No such file*, reboot the VNMC VM via vCenter.

Managing Backup Operations

We recommend that you use backup and restore operation as a disaster recovery mechanism. To migrate configuration data from one VNMC server to another, use export and import operations.

Creating a Backup Operation

Before You Begin

Obtain the backup server IP address or hostname and authentication credentials.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Click **Create Backup Operation**.

Step 3 In the Create Backup Operation dialog box, complete the following fields, then click **OK**:

Field	Description
Admin State	One of the following administrative states: • enabled—Backup is enabled. The system runs the backup operation when you click **OK**. • disabled—Backup is disabled. The system does not run the backup operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Type	Backup type. The backup creates a copy of the whole database file. You can use this file for disaster recovery if you need to recreate every configuration on your system. This field is not editable.
Protocol	Protocol used when communicating with the remote server: **Note** Do not use TFTP for backup and restore operations. • FTP • SCP • SFTP • TFTP
Hostname/IP Address	Hostname or IP address of the device where the backup file is stored. This entry cannot be changed when editing the operation. **Note** If you use a hostname instead of an IP address, you must configure a DNS server.

Field	Description
User	Username the system uses to log into the remote server. This field is not displayed if you select **TFTP** in the Protocol field.
Password	Password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. This field is not displayed if you choose **TFTP** in the Protocol field. **Note** VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File	Full path of the backup filename. This entry must start with a slash (/) and must not contain a relative path.

Running a Backup Operation

Procedure

Step 1 Choose **Administration > Operations > Backups >** *Backup-server* where *backup-server* is the server on which the backup file is stored.

Step 2 In the General tab, enter the following information:

a) In the Admin State field, choose **enabled**.
b) For all protocols except TFTP, in the Password field, enter the password for the identified user.
c) (Optional) Change the content of the other available fields.

Step 3 Click **Save**.
VNMC takes a snapshot of the configuration type that you selected and uploads the file to the network location.

Step 4 (Optional) To view the progress of the backup operation, click the **Task** tab. The Task tab provides the information described in the following table. The operation continues to run until it is completed.

Field	Description
Description	Task description.

Field	Description
Status	Task status.
Stage Descriptor	Description of the current stage.
Tries	Number of times the task has been tried.
Previous Status	Previous task status.
Remote Err Code	Remote error code.
Remote Err Description	Description of the remote error.
Remote Inv Result	Remote error result.
Time Stamp	Date and time when the task completed.
Progress	Progress of the current task, indicated by the percent complete, a progress bar, or both.

Editing a Backup Operation

Before You Begin

Obtain the backup server IP address or hostname and authentication credentials.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Select the backup operation you want to edit, then click **Edit**.

Step 3 In the Edit Backup dialog box, modify the information as required, then click **OK**.

Field	Description
Admin State	One of the following administrative states: • enabled—Backup is enabled. The system runs the backup operation when you click **OK**. • disabled—Backup is disabled. The system does not run the backup operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.

Field	Description
Type	Backup type. The backup creates a copy of the whole database file. You can use this file for disaster recovery if you need to recreate every configuration on your system. This field is not editable.
Protocol	Protocol used when communicating with the remote server: **Note** Do not use TFTP for backup and restore operations. • FTP • SCP • SFTP • TFTP
Hostname/IP Address	Hostname or IP address of the device where the backup file is stored. This entry cannot be changed when editing the operation. **Note** If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server. This field is not displayed if you select **TFTP** in the Protocol field.
Password	Password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. This field is not displayed if you choose **TFTP** in the Protocol field. **Note** VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File	Full path of the backup filename. This entry must start with a slash (/) and must not contain a relative path.

Deleting a Backup Operation

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Select the backup operation you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Restoring a Backup Configuration

Procedure

Step 1 Install the VNMC virtual machine. For information, see the *Cisco Virtual Network Management Center 2.0 Quick Start Guide*.

Step 2 Uninstall the VSG policy agents. Connect the Secure Shell to the VSG console for this task. This step does not cause a traffic disruption.

Example:
```
vsg# conf t
vsg (config)# vnmc-policy-agent
vsg (config-vnmc-policy-agent)# no policy-agent-image
```
Note Perform this step for all VSGs that are associated with the VNMC that you are restoring.

Step 3 Disable the ASA 1000V policy agent.

Example:
```
ASA-154# conf t
ASA-154(config)# no vnmc policy-agent
```

Step 4 Uninstall the VSM policy agents. Connect the Secure Shell to the VSM console for this task. This step does not cause a traffic disruption.

Example:
```
vsm# conf t
vsm (config)# vnmc-policy-agent
vsm (config-vnmc-policy-agent)# no policy-agent-image
```
Note Perform this step for all VSMs that are associated with the VNMC you are restoring.

Step 5 Restore the VNMC database. Connect the Secure Shell to the VNMC CLI for this task. Depending upon your VNMC backup location, restore using FTP, SCP, or SFTP.

Example:
```
vnmc# connect local-mgmt
vnmc(local-mgmt)# restore scp://username@server/path
```

Step 6 In the VNMC UI, choose **Administration > Service Registry > Clients**, and in the General tab, do the following:

a) Wait until each registered VSM displays the operational status as lost-visibility.

b) Choose each VSM, and click **Delete Client**.

Step 7 In the VNMC UI, choose **Resource Management > Resources > Virtual Supervisor Modules**, and verify that the deleted VSMs are not visible.

Step 8 Reregister the VSMs associated with VNMC by entering the following commands for each VSM:

Example:
```
VSM# conf t
VSM (config)# vnmc-policy-agent
VSM (config-vnmc-policy-agent)# registration-ip vsm-ip-address
VSM (config-vnmc-policy-agent)# shared-secret password
```

Step 9 Reinstall the VSM policy agents.

Note If the VSM policy agents must be upgraded, install the new software now.

Example:
```
VSM# conf t
VSM (config)# vnmc-policy-agent
VSM (config-vnmc-policy-agent)# policy-agent-image bootflash:vnmc-vsmpa.1.0.1g.bin
```

Step 10 Wait until all the VSMs have registered in the Service Registry and are displayed under **Resource Management > Resources > Virtual Supervisor Modules**.

Step 11 Reregister the VSGs associated with VNMC by entering the following commands for each VSG:

Example:
```
VSG# conf t
VSG (config)# vnmc-policy-agent
VSG (config-vnmc-policy-agent)# registration-ip vsg-ip-address
VSG (config-vnmc-policy-agent)# shared-secret password
```

Step 12 Reinstall the VSG policy agents.

Note If the VSG policy agents must be upgraded, install the new software now.

Example:
```
VSG# conf t
VSG (config)# vnmc-policy-agent
VSG (config-vnmc-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.1.0.1g.bin
```

Step 13 Re-enable the ASA 1000V policy agent.

Example:
```
ASA-154# conf t
ASA-154(config)# vnmc policy-agent
ASA-154(config-vnmc-policy-agent)# shared-secret password
ASA-154(config-vnmc-policy-agent)# registration host host-ip-address
```

Step 14 Verify the following states after the restore process is complete:

Note The restore process could take a few minutes depending upon your setup environment.

a) Using the VSG CLI, verify that your configurations are restored to their earlier state.
b) Using the VNMC UI, verify that your objects and policies are restored to their earlier state.
c) Using the ASA 1000V CLI, verify that your configurations are restored to their earlier state.

Managing Export Operations

Use export and import operations to migrate data from one VNMC server to another. To back up and restore VNMC data (for example, as a disaster recovery mechanism), use backup and restore operations.

Creating an Export Operation

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials before performing an export.

Note The associations of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in export or import data. Only firewall definitions are included, such as device profiles and policies. If an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Click **Create Export Operation**.

Step 3 In the Create Export Operation dialog box, provide the required information as described in the following table, then click **OK**:

Field	Description
Admin State	One of the following administrative states: • enabled—Export is enabled. The system runs the export operation when you click **OK**. • disabled—Export is disabled. The system does not run the export operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.

Field	Description
Type	One of the following export types: • config-all • config-logical • config-system
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP • TFTP
Hostname/IP Address	Hostname or IP address of the device where the export file is stored. This entry cannot be changed when editing the operation. **Note** If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server. This field is not displayed if you choose **TFTP** in the Protocol field.
Password	The password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. This field is not displayed if you choose **TFTP** in the Protocol field. **Note** VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the export operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Editing an Export Operation

Note The associations of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in export or import data. Only firewall definitions are included, such as device profiles and policies. If an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials before performing an export.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 In the Backups table, select the export operation you want to edit, then click **Edit**.

Step 3 In the Edit Export dialog box, modify the fields as appropriate, then click **OK**.

Field	Description
Admin State	One of the following administrative states: • enabled—Export is enabled. The system runs the export operation when you click **OK**. • disabled—Export is disabled. The system does not run the export operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Type	One of the following export types: • config-all • config-logical • config-system
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP • TFTP

Field	Description
Hostname/IP Address	Hostname or IP address of the device where the export file is stored. This entry cannot be changed when editing the operation. **Note** If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server. This field is not displayed if you choose **TFTP** in the Protocol field.
Password	The password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. This field is not displayed if you choose **TFTP** in the Protocol field. **Note** VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the export operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Deleting an Export Operation

Procedure

Step 1 In the Navigation pane, choose **Administration > Operation > Backups.**

Step 2 In the **Work** pane, click the export operation you want to delete.

Step 3 In the Confirm dialog box, click **Yes**.

Configuring Import Operations

Creating an Import Operation

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials.

Note The association of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in the export or import data. Only the compute and edge firewall definitions are included, such as device profiles and policies. Therefore, if an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Caution When the configuration data is imported into the VNMC server, you might see an error message and get logged out, followed by the display of a new VNMC certificate. This error occurs because the VNMC hostname, domain name, or both have changed. The VM Manager Extension needs to be exported again and installed on vCenter. To continue with the import, accept the VNMC certificate and log into VNMC again.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Click **Create Import Operation**.

Step 3 In the Create Import Operation dialog box, provide the following information as required, then click **OK**:

Field	Description
Admin State	One of the following administrative states: • enabled—Import is enabled. The system runs the import operation as soon as you click **OK**. • disabled—Import is disabled. The system does not run the import operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Action	Action to be taken on a file: merge.

Field	Description
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP • TFTP
Hostname/IP Address	Hostname or IP address of the device where the import file is stored. This entry cannot be changed when editing the operation. **Note** If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. This field does not appear if you choose **TFTP** in the Protocol field.
Password	Password the system uses to log into the remote server. This field does not appear if you choose **TFTP** in the Protocol field. **Note** VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the import operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Editing an Import Operation

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Select the import operation that you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, modify the fields as required, then click **OK**.

Field	Description
Admin State	One of the following administrative states: • enabled—Import is enabled. The system runs the import operation as soon as you click **OK**. • disabled—Import is disabled. The system does not run the import operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Action	Action to be taken on a file: merge.
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP • TFTP
Hostname/IP Address	Hostname or IP address of the device where the import file is stored. This entry cannot be changed when editing the operation. **Note** If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. This field does not appear if you choose **TFTP** in the Protocol field.

Field	Description
Password	Password the system uses to log into the remote server. This field does not appear if you choose **TFTP** in the Protocol field. **Note** VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the import operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Deleting an Import Operation

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Select the import operation that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

INDEX

A

AAA policies 139
  configuring 139
ACL policies 78
  adding 78
ACL policy rules, and time ranges 82
ACL policy sets 84
  adding 84
Add ACL Policy Rule dialog box 78
Add Auth Policy dialog box 140
Add Compute Security Profile dialog box 114
Add Connection Timeout Policy Rule dialog box 85
Add Data Interface dialog box 183
Add DHCP Server Policy dialog box 88
Add Edge Firewall dialog box 183
Add Edge Security Profile dialog box 118
Add Interface Policy Set dialog box 105
Add IP Audit Policy Rule dialog box 90
Add NAT Policy Rule dialog box 93
Add NTP Server dialog box 171
Add Policy to Authenticate Peer dialog box 109
Add Syslog Policy dialog box 154
Add Syslog Server dialog box 160
adding 38, 40, 43, 46, 52, 59, 62, 64, 78, 84, 86, 125, 126, 129, 130, 133, 142, 144, 147, 150, 154, 160, 165, 177, 182, 183, 190
  ACL policies 78
  ACL policy sets 84
  compute firewalls 177
  connection timeout policies 84
  core file policies 38, 142
  data interfaces 183
  DHCP relay servers 86
  DNS servers 59
  edge firewalls 182
  fault policies 40
    VNMC profile 40
  fault policy 144
    device profile 144
  firewall device profiles 165
  logging policies 43
    VNMC profile 43
adding *(continued)*
  logging policy 147
    device profile 147
  object group expressions 126
  object groups 125
  pools 190
  security profile dictionary 129
  security profile dictionary attributes 130
  SNMP community 150
  SNMP policies 150
  SNMP trap 150
  syslog policies 46, 154
    device profile 154
    VNMC profile 46
  syslog server 52
    VNMC profile 52
  syslog servers for devices 160
  VM Managers 62, 64
  vZones 133
adding an SNMP trap receiver 153
administrative operation 193
  conventions 193
applying 119, 120
  edge device profiles 119
  edge security profiles 120
ASA 1000V firewalls, overview 177
ASA 1000Vs 184, 185
  assigning 184
  unassigning 185
ASDM 187
  launching 187
assigning 125, 181, 191
  policy 125
  pool 191
  VSGs 181
associating 172
  device policies 172

B

backing up 194
  VNMC 194
backup operations 193
  managing 193

C

changing 32
  locales 32
  roles 32
clone 11
compute firewalls 172, 177, 178, 186
  adding 177
  applying device profiles 172
  editing 178
  examining faults 186
compute security profiles 113
  configuring 113
configuring 86, 89, 90, 91, 92, 95, 96, 97, 98, 99, 100, 103, 105, 106, 109, 110, 113, 115, 117, 139, 170
  AAA policies 139
  compute security profiles 113
  crypto map policies 100
  device policies 139
  device profiles 170
  DHCP policies 86
  edge device profiles 115
  edge security profiles 117
  IKE policies 103
  interface policy sets 105
  IP audit policies 89, 90
    configuring 90
  IP audit signature policies 91
  IPsec policies 106
  NAT policy sets 95
  NAT/PAT policies 92
  NTP 170
  packet inspection policies 97
  PAT 96
  PAT for edge firewalls 95, 96
  peer authentication policies 109
  routing policies 98
  TCP intercept policies 99
  VPN device policies 110
  VPN policies 100
connection timeout policies 84
  adding 84
conventions 193
  administrative operations 193
creating 14, 24, 26, 28, 35, 70, 72, 73, 74, 194, 200, 204
  applications 73
creating *(continued)*
  backups 194
  export operations 200
  import operations 204
  LDAP provider 14
  locales 26
  tenants 70
  tiers 74
  trusted points 35
  user accounts 28
  user roles 24
  virtual data centers 72
crypto map policies 100
  configuring 100

D

data interfaces 183
  adding 183
deleting 17, 25, 27, 28, 36, 40, 43, 45, 51, 56, 59, 60, 64, 67, 71, 73, 74, 75, 124, 128, 129, 132, 135, 143, 146, 149, 152, 154, 160, 165, 170, 181, 192, 198, 203, 207
  application 74
  backup operation 198
  compute firewalls 181
  core file policies 40
    VNMC profile 40
  core file policy 143
    device profile 143
  DNS server 59
  export operation 203
  fault policy 43, 146
    device profile 146
    VNMC profile 43
  firewall device profile 170
  import operation 207
  LDAP provider 17
  locales 27
  logging policies 45
    VNMC profile 45
  logging policy 149
    device profile 149
  NTP server 60
  object group expressions 129
  object groups 128
  organizations from a locale 28
  pool 192
  security profile 124
  security profile attribute 124
  security profile dictionary 132
  security profile dictionary attribute 132
  SNMP policy 152

deleting *(continued)*
SNMP trap receiver 154
syslog policy 51, 160
device profile 160
VNMC profile 51
syslog server 56, 165
device profile 165
VNMC profile 56
tenants 71
tiers 75
trusted points 36
user roles 25
deleting 25
virtual data center 73
VM Manager 64, 67
vZone conditions 135
vZones 135
device configuration 138
device policies 137, 139, 172
associating with profiles 172
configuring 139
device profiles 137, 170, 172
applying to compute firewalls 172
applying to edge firewalls 172
configuring 170
DHCP policies 86
configuring 86
DHCP relay policies 87
configuring 87
DHCP relay policies 87
DHCP relay servers 86
adding 86
DNS server 59
deleting 59

E

Edge Device Profile dialog box 116
edge device profiles 115, 119
applying 119
configuring 115
edge firewall security profiles 122
configuring 122
edge firewalls 172, 182, 184, 185, 186
adding 182
applying device profiles 172
assigning ASA 1000Vs 184
examining faults 186
unassigning ASA 1000Vs 185
edge security profiles 117, 120
applying 120
configuring 117
Edit Security Profile Dictionary dialog box 131
editing 16, 25, 27, 36, 39, 41, 44, 48, 54, 56, 60, 63, 65, 71, 72, 74, 75, 121, 122, 127, 128, 131, 134, 143, 145, 148, 151, 153, 163, 167, 178, 191, 196, 202, 205
application 74
backup operations 196
compute firewalls 178
core file policies 39
VNMC profile 39
core file policy 143
device profile 143
default VNMC profile 56
DNS domains 60
export operation 202
fault policies 41
VNMC profile 41
fault policy 145
device profile 145
firewall device profiles 167
import operations 205
LDAP provider 16
locales 27
logging policies 44
VNMC profile 44
logging policy 148
device profile 148
object group expression 128
object groups 127
pools 191
security profile dictionary attribute 131
security profiles 121, 122
SNMP policy 151
SNMP trap receiver 153
syslog policies 48
VNMC profile 48
syslog policy 48
local destinations 48
syslog server 54
VNMC profile 54
syslog servers 163
tenants 71
tiers 75
trusted points 36
user roles 25
virtual data centers 72
VM Manager 63, 65
vZones 134
export operations 200
managing 200

F

faults 185, 186
  compute firewalls 186
  edge firewalls 186
  viewing details 185
field aids 8
firewall access 5
firewall device profiles 167
  editing 167
firewalls, using 5

H

Hyper-V Hypervisor 9

I

IKE policies 103
  configuring 103
IKE V1 Policy dialog box 104
IKE V2 Policy dialog box 104
interface policy sets, configuring 105
IP audit signature policies 91
  configuring 91
IPsec IKEv1 Proposal dialog box 107, 108
IPsec policies 106
  configuring 106

L

launching 187
  ASDM 187
LDAP provider 14, 16, 17
  creating 14
  deleting 17
  editing 16
locales 26, 27, 28
  assigning organizations 28
  creating 26
  editing 27
locally authenticated user account 32
  changing locales 32
  changing roles 32
logging in 6

M

managed resources 175
managing 193, 200
  backup operations 193
  export operations 200
monitoring 32
  user sessions 32
multi-tenant environments 69

N

name resolution 70
NAT policy sets 95
  configuring 95
NAT/PAT policies 92
  configuring 92
New DHCP Relay Policy dialog box 87
New DHCP Relay Server dialog box 87
NTP 59, 170
  configuring 170
  configuring for VNMC 59

O

object groups 125, 127
  adding 125
  editing 127
organizations 26
  creating locales 26
overview 61
  VM Managers 61

P

packet inspection policies 97
  configuring 97
passwords 20
  guidelines 20
PAT 95, 96
  configuring 95, 96
peer authentication policies 109
  configuring 109
policies 37, 115, 120, 138, 139
  configuring 139
  verifying 115, 120
  VNMC profile 37
pools 191, 192
  assigning 191
  unassigning 192
profiles 37, 113, 115, 117, 119, 120, 172
  applying 119, 120, 172
  configuring 113, 115, 117, 172

profiles *(continued)*
types of 113

R

registration 185
verifying 185
Remote Access Method dialog box 141
remote authentication 13
providers 13
resource management 175
Resource Manager 176
restoring 198
backup configuration 198
VNMC software 198
routing policies 98
configuring 98
running 195
backups 195

S

Search 10
security policies 137
security profiles 122
configuring 122
selecting 17
primary authentication service 17
service policies 77
configuring 77
service policies 77
setting 9
inactivity timeout 9
syslog policy 157
device profile 157

T

TCP intercept policies 99
configuring 99
tenant management 69
tenants 70
creating 70
time ranges in ACL policy rules 82
toolbar 8
trusted points 35

U

unassigning 125, 182, 192
policy 125
pools 192
VSGs 182
user accounts 19
user interface 6
user locales 23
user privileges 22
user roles 21
usernames 20
guidelines 20

V

verifying 115, 120, 185
compute firewall policies 115
edge firewall policies 120
VM registration 185
virtual machines 176
Virtual Security Gateways 176
VM Manager 62
adding 62
VM Managers 61, 64
adding 64
overview 61
VMs 185
verifying registration 185
VNMC 59, 194
backing up 194
configuring NTP 59
VPN device policies 110
configuring 110
VPN policies 100
configuring 100
VSGs 176, 182
unassigning pools 182
vZones 133
adding 133
vZones, overview 132