vGW Series Infrastructure Protection

Published: 2015-02-19

Copyright © 2015, Juniper Networks, Inc.

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

vGW Series Infrastructure Protection
Copyright © 2015, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation . . . xiii
Documentation and Release Notes . . . xiii
Documentation Conventions . . . xiii
Documentation Feedback . . . xv
Requesting Technical Support . . . xvi
Self-Help Online Tools and Resources . . . xvi
Opening a Case with JTAC . . . xvi

Part 1 Network and Firewall

Chapter 1 **Network Module . . . 3**

Understanding the vGW Series Network Module . . . 3
Network Module . . . 3
Manipulating Displayed Information . . . 4
Changing the Time Interval for Displayed Information . . . 5
Using Advanced Options for Filtering Network Data . . . 7
Sorting Table Data . . . 7
Using the vGW Series Network and Firewall Modules Cooperatively . . . 8
Network Assessment . . . 8
Using the Network Module to Observe Traffic Coming Into and Going Out from VMs . . . 9
Detecting Unexpected and Unwanted Behavior . . . 9
Using the Network and Firewall Modules Together . . . 10

Chapter 2 **Firewall Module . . . 11**

Understanding the vGW Series Firewall Module . . . 11
The Firewall Module and the VM Tree . . . 11
Overview of the Firewall Policy Model . . . 12
Global Policy, Group Policy, and Individual VM Policy Tiers . . . 13
Global Policy . . . 13
Group Policy . . . 15
Individual VM Policy Rules . . . 15
Default Policy . . . 16
Quarantine Policy . . . 16
Firewall Policy Structure and Policy Rules Precedence . . . 16
Viewing the Complete Policy Rule Base for a VM . . . 18
The Manage Policy Tab . . . 18
Policy Per vNIC and Dual Stack . . . 19
Creating a Policy Rule . . . 19
The Apply Policy Tab . . . 22

The Logs Tab . . . 23
Understanding How vGW Series Handles ICMPv6 Protocol Traffic . . . 24
About ICMPv6 . . . 25
Filtering ICMPv6 Packets . . . 25
Default Policy Group for Allowing Inbound ICMPv6 Packets . . . 26
Viewing the Default ICMPv6 Protocols Group Members . . . 26
Editing the Default ICMPv6 Protocols Group Members . . . 27
Understanding Predefined Objects for vGW Series Firewall Policy Terms . . . 28
Defining and Selecting Source and Destination Terms for Policy Rules . . . 28
Predefined Global IP Address Objects . . . 29
Predefined Network Objects . . . 29
Predefined Network Objects for Well Known IP Addresses . . . 30
Additional IPv4 and IPv6 Predefined Network Objects . . . 30
Configuring vGW Series Firewall Policies . . . 32
Understanding vGW Series Predefined Firewall Policy for Its Components . . . 38

Part 2 IDS and AntiVirus

Chapter 3 **IDS Module . . . 41**

Understanding the vGW Series IDS Module . . . 41
Managing and Sorting Displayed Alerts Information . . . 41
Top Alerts Page . . . 42
Alert Sources Page . . . 47
Alert Targets Page . . . 47
All Alerts Page . . . 47
Configuring IDS Settings and Viewing Activity . . . 48

Chapter 4 **AntiVirus Module Basics . . . 51**

Understanding vGW Series AntiVirus . . . 51
About Antivirus Software . . . 52
Signature-Based Detection . . . 52
The vGW AntiVirus Feature . . . 52
The vGW AntiVirus Dashboard . . . 54
vGW AntiVirus Configuration Overview . . . 58
Understanding Quarantined VMs and How to Manage Them . . . 65
About vGW Series Quarantine . . . 65
Configuring a Quarantine Policy . . . 66
Viewing the Quarantined VMs, Releasing Them From Quarantine, and Resolving Problems . . . 67

Chapter 5 **vGW Endpoint for AntiVirus . . . 69**

Understanding and Installing the vGW Endpoint . . . 69
Installing the vGW Endpoint . . . 69
vGW AntiVirus Endpoint Auto-Update . . . 69
vGW Endpoint on the VM . . . 70
Quarantined Files . . . 72
vGW Endpoint Components and Displays . . . 72
vGW Endpoint Behavior . . . 73

 Copyright © 2015, Juniper Networks, Inc.

Chapter 6 AntiVirus Scanning Config 75
Configuring vGW Series AntiVirus On-Access Scanning 75
Configuring vGW Series AntiVirus On-Demand Scanning 78

Part 3 Introspection

Chapter 7 Introspection Module Basics 85
Understanding the vGW Series Introspection Module 85

Chapter 8 Introspection Software Monitoring 87
Understanding the vGW Series Introspection Applications Tab 87
Understanding the vGW Series Introspection VMs Tab 90

Chapter 9 Image Enforcer and Enforcer Profiles 93
Understanding the vGW Series Introspection Image Enforcer Feature 93
Understanding the vGW Series Image Enforcer Tab 94
Understanding the vGW Series Enforcer Profiles Tab 95
About the Enforcer Profiles Screen 96
The Add Enforcer Profile Pane 96

Chapter 10 Scans and Scheduling Scans 101
Understanding the vGW Series Introspection Scheduling Feature 101
Understanding the vGW Series Introspection Scan Status 102

Chapter 11 Registry Inspection 105
Understanding the vGW Series Introspection Registry Check Feature 105
Configuring the vGW Series Introspection Registry Feature 106

Part 4 Quarantine

Chapter 12 Quarantined VMs 113
Understanding Quarantined VMs and How to Manage Them 113
About vGW Series Quarantine 113
Configuring a Quarantine Policy 114
Viewing the Quarantined VMs, Releasing Them From Quarantine, and Resolving Problems 115

Part 5 Compliance

Chapter 13 Compliance Module and Hypervisor 119
Understanding the vGW Series Compliance Module 119
The Compliance Module 119
The Compliance Tab 120
The Rules Tab 121
Configuring a Compliance Rule 121
Understanding the vGW Series Hypervisor and Extended VM Security 124
The Need for Hypervisor Security 125
vGW Series Hypervisor and VM Security, and VMware Hardening Guidelines 125
vGW Series Hypervisor and VM Security Overview 125
Remediation 126

Copyright © 2015, Juniper Networks, Inc.

Configuration Example 126

Part 6 Index

Index 131

Copyright © 2015, Juniper Networks, Inc.

List of Figures

Part 1 Network and Firewall

Chapter 1 Network Module 3

Figure 1: Network Summary Tab for All VMs 4
Figure 2: Main Module Network Module Summary Tab for a Single VM 4
Figure 3: Displaying Network Data for Different Time Intervals: Part 1 5
Figure 4: Displaying Network Data for Different Time Intervals: Part 2 5
Figure 5: Selecting a Time Interval 6
Figure 6: Setting the Custom Time Period 6
Figure 7: Top Protocols Across All Machines Example 8
Figure 8: Network Module Connection Tab Information 9

Chapter 2 Firewall Module 11

Figure 9: Firewall Module Policy for a Single VM 12
Figure 10: Global Policy 15
Figure 11: VM Policy Expanded Rule Base 18
Figure 12: Firewall Module Manage Policy Page 19
Figure 13: Adding a Rule 20
Figure 14: Using the Dialog Box Filter to Add Terms for policy rules 20
Figure 15: Firewall Apply Policy Page 22
Figure 16: Firewall Module Logs Tab 24
Figure 17: Default Global Policy Showing Default ICMPv6 Allow Group 26
Figure 18: Protocols Settings ICMPv6 Default Protocol Group 26
Figure 19: Default Global Policy 33
Figure 20: Adding a Global Policy Rule to Reject Telnet Connection Attempts . . . 34
Figure 21: VM Policy for an Individual VM 36
Figure 22: Complete VM Policy for an Individual VM 36

Part 2 IDS and AntiVirus

Chapter 3 IDS Module 41

Figure 23: IDS Top Alerts 42
Figure 24: IDS Top Alerts Advanced Options 43
Figure 25: IDS Alert Description 44
Figure 26: IDS Alert Details 44
Figure 27: IDS Alert Details Showing Affected Systems 45
Figure 28: IDS Alert Sources 46
Figure 29: IDS Alert Targets 46
Figure 30: IDS All Alerts 47
Figure 31: IDS Settings Page 48

Chapter 4 AntiVirus Module Basics 51

Figure 32: vGW AntiVirus Dashboard 55
Figure 33: Virus Alerts 56
Figure 34: vGW AntiVirus Scanner Config Tab 57
Figure 35: Quarantined Files 57
Figure 36: On-Access Scan 60
Figure 37: vGW AntiVirus Dashboard 62
Figure 38: Scanner Config Tab 63
Figure 39: Quarantine Policy in the VM Tree 66
Figure 40: Configuring a vGW Series Quarantine Policy 67
Figure 41: Main Module Quarantine Tab 67

Chapter 5 **vGW Endpoint for AntiVirus 69**

Figure 42: vGW AntiVirus Settings 70
Figure 43: vGW AntiVirus Endpoint Connection Process Dialog Box 71
Figure 44: vGW AntiVirus Endpoint Threat Detection Dialog Box 71

Chapter 6 **AntiVirus Scanning Config 75**

Figure 45: Scanner Config Tab 80
Figure 46: Step 2: Scan Schedule 80

Part 3 Introspection

Chapter 8 **Introspection Software Monitoring 87**

Figure 47: vGW Series Introspection Module Applications Tab 87
Figure 48: vGW Series Introspection Module VMs Tab 90

Chapter 9 **Image Enforcer and Enforcer Profiles 93**

Figure 49: vGW Series Introspection Module Image Enforcer Tab 95
Figure 50: vGW Series Introspection Module Enforcer Profiles Tab 96
Figure 51: Adding a vGW Series Introspection Module Image Enforcer Profile 97

Chapter 10 **Scans and Scheduling Scans 101**

Figure 52: Introspection Module Scheduling Page 101
Figure 53: vGW Series Introspection Module Scan Status Page 103

Chapter 11 **Registry Inspection 105**

Figure 54: Configuring a New Registry Key 107
Figure 55: Add Schedule for Scan Page 108
Figure 56: Add an Enforcer Profile that Allows for Registry Scans 108

Part 4 Quarantine

Chapter 12 **Quarantined VMs 113**

Figure 57: Quarantine Policy in the VM Tree 114
Figure 58: Configuring a vGW Series Quarantine Policy 115
Figure 59: Main Module Quarantine Tab 115

Part 5 Compliance

Chapter 13 **Compliance Module and Hypervisor 119**

Figure 60: vGW Series Compliance Module 120
Figure 61: vGW Series Compliance Module Rules Tab 121

 Copyright © 2015, Juniper Networks, Inc.

Figure 62: Adding a Predefined Compliance Rule 124

Copyright © 2015, Juniper Networks, Inc.

List of Tables

About the Documentation xiii

Table 1: Notice Icons xiv
Table 2: Text and Syntax Conventions xiv

Part 1 Network and Firewall

Chapter 1 Network Module 3

Table 3: Using Advanced Options for Filtering Network Data 7

Chapter 2 Firewall Module 11

Table 4: Firewall Policy Configuration Settings 21
Table 5: Firewall Policy Icons 23

Part 3 Introspection

Chapter 9 Image Enforcer and Enforcer Profiles 93

Table 6: Add Enforcer Profile: Selecting the Gold Image and VMs to Be Compared Against It 97
Table 7: Edit Enforcer Profile Options 98
Table 8: VM Gold Image Allowed Deviations 98
Table 9: Actions 99
Table 10: Compliance Rule Specifications 99

Chapter 10 Scans and Scheduling Scans 101

Table 11: Scan Definition Options 101

Part 5 Compliance

Chapter 13 Compliance Module and Hypervisor 119

Table 12: Compliance Rule Creation Parameters 122

Copyright © 2015, Juniper Networks, Inc.

About the Documentation

- Documentation and Release Notes on page xiii
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xvi

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Documentation Conventions

Table 1 on page xiv defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xiv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Copyright © 2015, Juniper Networks, Inc.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

Copyright © 2015, Juniper Networks, Inc.

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

Copyright © 2015, Juniper Networks, Inc.

PART 1

Network and Firewall

- Network Module on page 3
- Firewall Module on page 11

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 1

Network Module

- Understanding the vGW Series Network Module on page 3
- Using the vGW Series Network and Firewall Modules Cooperatively on page 8

Understanding the vGW Series Network Module

The vGW Security Design VM Network module displays network traffic for virtual machines (VMs) that are selected in the VM tree. You can view network traffic for all VMs or specific ones.

This topic includes the following sections:

- Network Module on page 3
- Manipulating Displayed Information on page 4

Network Module

The Network module contains the following six tabs:

- Summary
- Top Protocols
- Top Sources
- Top Destinations
- Top Talkers
- Connections

To display information for a VM, the VM must have a known IP address. The IP address is determined automatically if VMware Tools is installed on the VM. If it is not set automatically, you can set the IP address manually using the Settings module vGW Application Settings > Machines page.

The Network module analysis takes into account IPv4 traffic and IPv6 traffic. Tables shown on the Network module tabs display information for objects with IPv4 and IPv6 addresses.

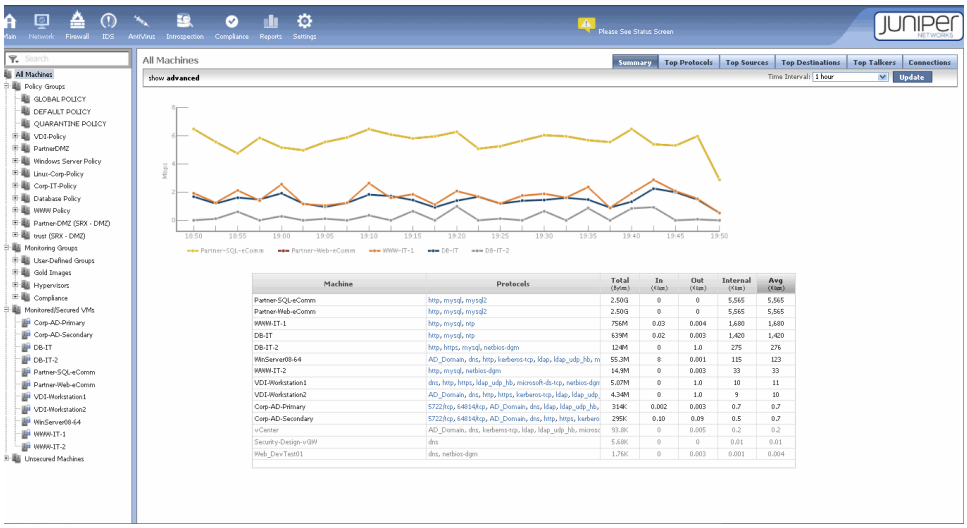
Copyright © 2015, Juniper Networks, Inc.

Manipulating Displayed Information

The Network Summary tab allows you to display information about all VMs, as shown in Figure 1 on page 4.

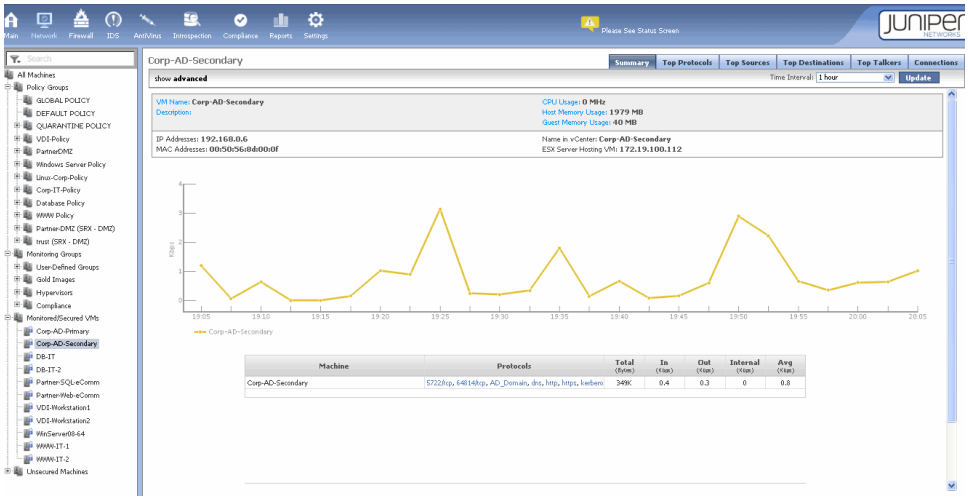
A line graph displayed at the top of the page plots bandwidth usage for the top VMs in the report. A table below the graph provides detailed network data for VMs selected in the VM tree. In this case, data for 1 hour is displayed.

Figure 1: Network Summary Tab for All VMs



To display information about a single VM, select the VM in the VM tree. Figure 2 on page 4 shows the information displayed for the Corp-AD-Secondary VM.

Figure 2: Main Module Network Module Summary Tab for a Single VM



To view a VM's connections, click an individual line in the graph. To display a filter for a protocol, click the protocol field.

Copyright © 2015, Juniper Networks, Inc.

Changing the Time Interval for Displayed Information

To change the period for which network data is plotted, use the Time Interval menu. Choose a different interval, and click **Update**. You can select a time interval or specify a custom period.

TIP: **The time interval feature is also available for other vGW Security Design modules.**

Figure 3 on page 5 and Figure 4 on page 5 show information for all machines for two different time periods.

Figure 3: Displaying Network Data for Different Time Intervals: Part 1

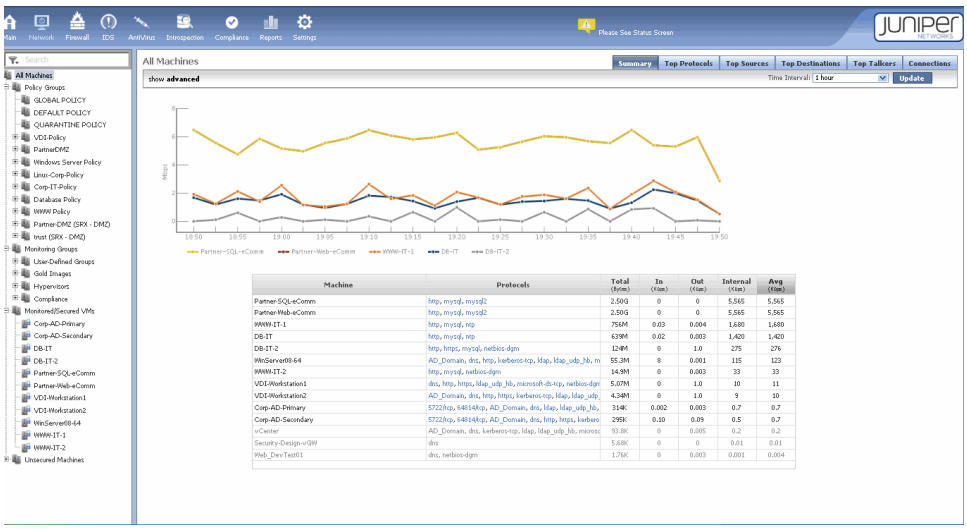
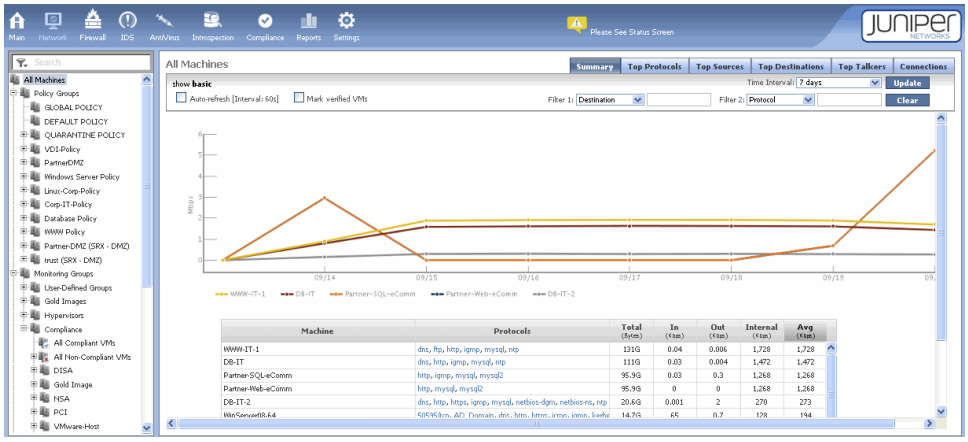


Figure 4: Displaying Network Data for Different Time Intervals: Part 2



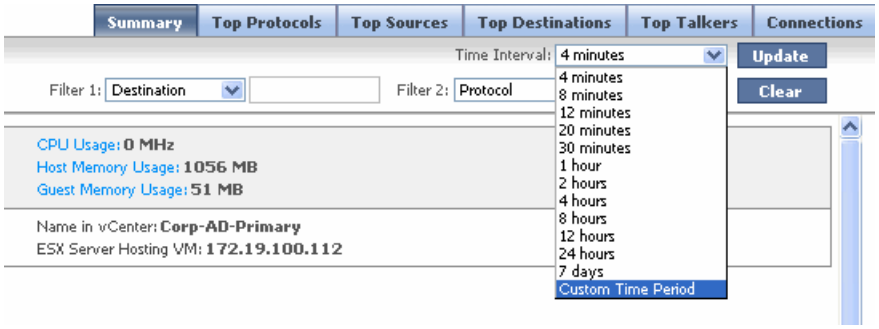
Real-time data from the last traffic interval populates the Total, In, Out, and Internal table columns. If you are charting protocols, sources, destinations, or top talkers, the interval selected is used to calculate the minimum, maximum, and average figures in the

Copyright © 2015, Juniper Networks, Inc.

table shown below the graph. For example, if you select 4 minutes as the time interval, the graph would show a sample of the throughput every 10 seconds. Each dot represents the average throughput value for that period.

The Custom Time Period feature allows you to view historical data. To use it, in the Time Interval menu, select **Custom Time Period**. (Figure 5 on page 6 shows the Custom Time Period menu item.)

Figure 5: Selecting a Time Interval



The custom time period is interpreted as follows:

- You can not set the custom time period to a range of less than 1 minute.

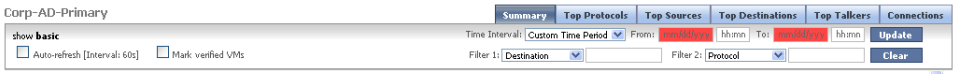
  If you enter the same value for the **From** and **To** fields—that is, the same beginning and end—vGW Series automatically changes the time interval to 1 minute before the specified time.

  For example, if you set the **From** field value to 01/02/13 00:00 and the **To** field value to 01/02/13 00:00, vGW Series changes the **From** time to 01/01/13 23:59 (11:59 P.M.) to allow for a time period of 1 minute. The **To** field is still interpreted as 01/02/13 00:00, the beginning of the next day.

- If you specify a valid time range, such as the **From** field set to 01/01/13 00:00 with the **To** field set to 01/02/13 00:00, vGW Series uses the time you specified.

Figure 6 on page 6 shows the Custom Time Period fields.

Figure 6: Setting the Custom Time Period



NOTE: Depending on the size of the database and the resources available to it, when you specify a custom time period, the vGW Security Design VM might take 30 minutes or more to chart the data and display it. When you want to examine a large data set, for example, data from a month or more, we recommend that you use the Reporting module.

Copyright © 2015, Juniper Networks, Inc.

Using Advanced Options for Filtering Network Data

You can filter the information to be displayed. To display filtering options, click **show advanced** at the left end of the time interval bar. Click the **Filter 1** and **Filter 2** menus to select filtering options and enter associated values in the related boxes. Then click **Update** to refresh the graph and data display, based on your settings. Click **Clear** to reset filter boxes.

NOTE: **Configured filters affect all data in the graph and tables.**

Other advanced options differ somewhat depending on the tab you are viewing. Table 3 on page 7 describes the Advanced options.

Table 3: Using Advanced Options for Filtering Network Data

Select	Action
Auto-refresh	Refreshes data automatically every 60 seconds.
mark verified VMs	Causes the vGW Series to automatically use the unique VMware ID/UUID as well as the IP address to validate that connections are actually coming from the identified server. vGW Series reports on both IPv4 and IPv6 addresses. Using both the VMware ID/UUID and the IP address protects against security threats such as IP spoofing. VMs for which this extra validation occurs can be displayed in the interface.
multicast in table	Includes multicast packets when monitoring. Because multicast packets are not destined for a specific host and they are seen by all machines on the network, they are included in the connection session list for all VMs. However, the amount of multicast traffic can be quite large, and it can obscure sessions specific to a selected VM. To remove multicast from this view, clear the **multicast in table** check box.

To exit advanced view, click **show basic**.

Sorting Table Data

You can sort table data in the Network page by column. Drag the pointer over the column headings. When the pointer changes to the pointing hand, click the column heading to sort.

To display information for a single VM that is listed in the table, click its entry.

Related Documentation

- Using the vGW Series Network and Firewall Modules Cooperatively on page 8
- *Understanding the vGW Security Design VM*
- *Understanding the vGW Security Design VM Taskbar*
- *About the vGW Security Design VM Tree*
- *Understanding vGW Series*

Copyright © 2015, Juniper Networks, Inc.

Using the vGW Series Network and Firewall Modules Cooperatively

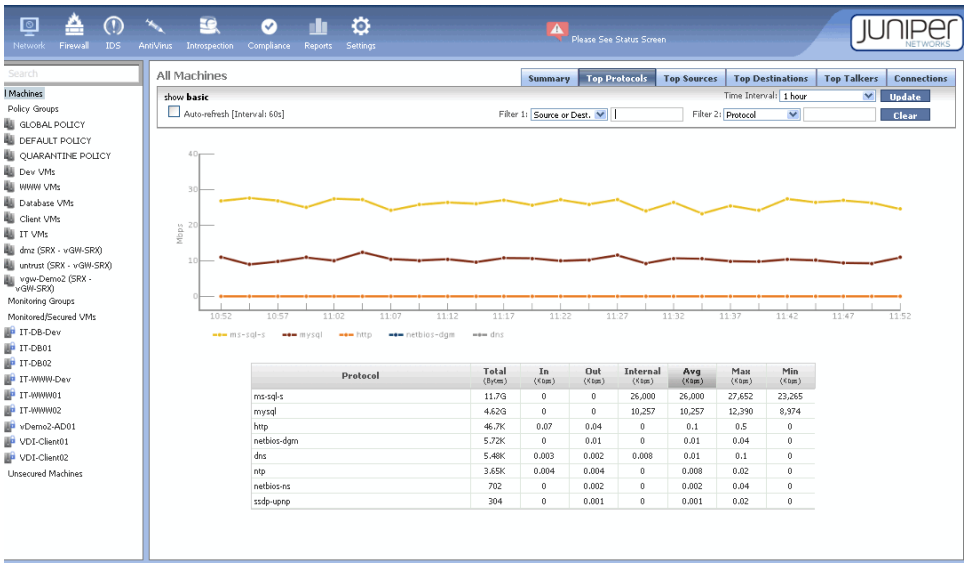
There are various ways to use the Network module in the service of the Firewall module to build a strong firewall. This topic explores some of them.

- Network Assessment on page 8
- Using the Network Module to Observe Traffic Coming Into and Going Out from VMs on page 9
- Detecting Unexpected and Unwanted Behavior on page 9
- Using the Network and Firewall Modules Together on page 10

Network Assessment

Administrators are not always aware of events that transpire on their virtualized networks because existing software for the virtualized environment does not always expose them. vGW Series Network module addresses this problem. It gives you a clear view of all traffic flows across your virtualized network. You can view overall throughput, chart protocol usage, identify sources and destinations of traffic, and identify top talkers. You can calculate minimum, maximum, and average figures across specific time intervals for these aspects of your network. In the example shown in Figure 7 on page 8, the Top Protocols assessment shows that the most heavily used protocols are Microsoft SQL Server followed by MySQL. The table beneath the graph gives details on all protocols used in top down order from most used to least.

Figure 7: Top Protocols Across All Machines Example



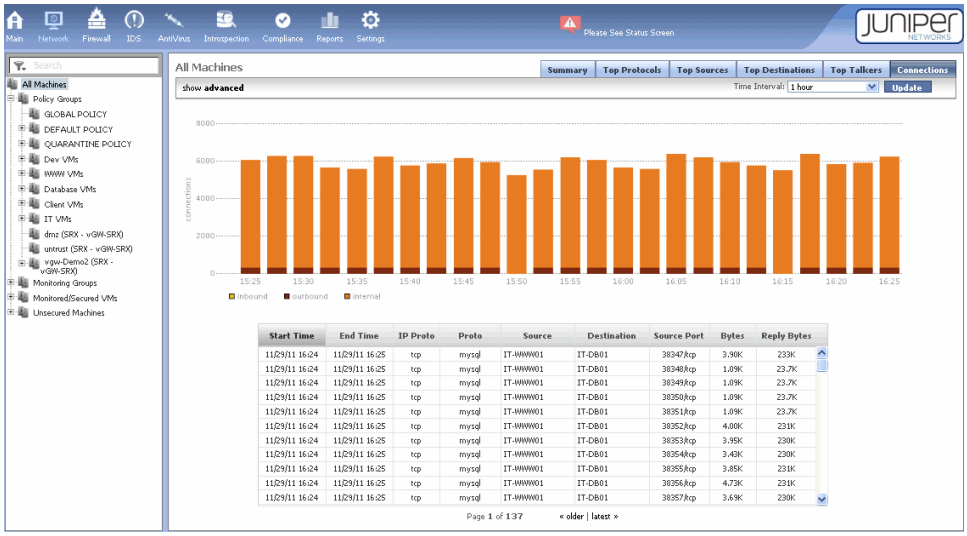
Protocol	Total (Bytes)	In (Kbps)	Out (Kbps)	Internal (Kbps)	Avg (Kbps)	Max (Kbps)	Min (Kbps)
ms-sql-s	11.7G	0	0	26,000	26,000	27,652	23,265
mysql	4.62G	0	0	10,257	10,257	12,390	8,974
http	46.7K	0.07	0.04	0	0.1	0.5	0
netbios-dgm	5.72K	0	0.01	0	0.01	0.04	0
dns	5.48K	0.003	0.002	0.008	0.01	0.1	0
ntp	3.65K	0.004	0.004	0	0.008	0.02	0
netbios-ns	702	0	0.002	0	0.002	0.04	0
ssdp-upnp	304	0	0.001	0	0.001	0.02	0

Because the vGW Series allows you to view activity that occurs inside the hypervisor, you can quickly discover who is communicating with whom. If you were to use only the vGW Series ability to view connections in real time, you would still be able to make realistic network assessments. But the vGW Series can contribute much more information to use in your network assessment.

Copyright © 2015, Juniper Networks, Inc.

As Figure 8 on page 9 shows, the Network module's Connections tab displays the number of connections in your network across time for all machines, whether the connections are inbound, outbound, or internal. The table beneath the graph shows when the connection was set up and when it ended, the protocol used, the source and destination endpoints, and the bytes transmitted. You can view this kind of information for an individual VM by selecting the VM in the VM tree.

Figure 8: Network Module Connection Tab Information



Using the Network Module to Observe Traffic Coming Into and Going Out from VMs

The Network module contributes to your ability to create strong firewall security in many ways. It displays information about all traffic, including traffic internal to a VM, traffic in and out of its vNICs, traffic from another VM on the same host, traffic between VMs on different hosts, and even traffic transmitted through a physical connection. In its simplest sense, you can think of this aspect of the Network module as akin to a packet sniffer, but it is far more than that.

When you use the Time Interval field to select a different time period, vGW Series redraws its graphs to let you view traffic patterns that occur during that period. You might want to use this feature to compare activity during one period of time with another, to look at past behavior, or to hone in on a VM to view its activity during a specific period.

For example, you could view all HTTP connections, the engaged workstations, and how much traffic is transmitted. You could do this for a two-day period, then a week, and then longer to observe anomalies that might exist.

Detecting Unexpected and Unwanted Behavior

The Network module can reveal unwanted behavior on your network that should be prohibited or investigated further. There are many examples of the kinds of information that the Network module might reveal. For example, you might notice that:

- Traffic might be transmitted on a particular protocol that is unusual or inappropriate, therefore raising questions.

  - The protocol 999TCP might be connecting to the finance server, an unwanted event that you want the firewall to protect against.
  - HTTP traffic might be transmitted to a VM that should not receive it.
- Some workstations might pull updates from a Microsoft server unintentionally instead of from local update servers.
- Thirty different protocols might be used, not all of which you were informed about. You might want to prohibit use of some of them.

Using the Network and Firewall Modules Together

When used together, the Network module and the Firewall module allow you to implement appropriate, strong security for your virtualized environment. By using the Network module to view how VMs behave in real time, you can better analyze your current security posture and observe its weaknesses.

As you begin to lock down your system through the Firewall module, the Network module becomes increasingly useful. After you use the Firewall module to refine your security policy, you can return to the Network module to determine if the change in policy produces the expected behavior.

You might still notice traffic that should not be allowed. In that case, you can return to the Firewall module, create a rule or modify an existing one, and then look at the behavioral results again in the Network module.

You can cycle through this process as many times as necessary to put in place the desired security policy. You can continue to use the Network module and the Firewall module together to implement the security you desire as your network expands and as its security requirements change.

Related Documentation

- Understanding the vGW Series Firewall Module on page 11
- Understanding the vGW Series Network Module on page 3
- *Understanding the vGW Security Design VM*
- *Understanding the vGW Security Design VM Taskbar*
- *About the vGW Security Design VM Tree*
- *Understanding vGW Series*

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 2

Firewall Module

- Understanding the vGW Series Firewall Module on page 11
- Understanding How vGW Series Handles ICMPv6 Protocol Traffic on page 24
- Understanding Predefined Objects for vGW Series Firewall Policy Terms on page 28
- Configuring vGW Series Firewall Policies on page 32
- Understanding vGW Series Predefined Firewall Policy for Its Components on page 38

Understanding the vGW Series Firewall Module

This topic covers the vGW Series Firewall module that allows you to create reusable and individual policy rules to use in building policies for groups of VMs and individual VMs. You also use the Firewall module to apply those policies to VMs.

Before it covers the Firewall module interface, this chapter explains the policy module concepts that are fundamental to constructing firewall policies.

This topic contains the following sections:

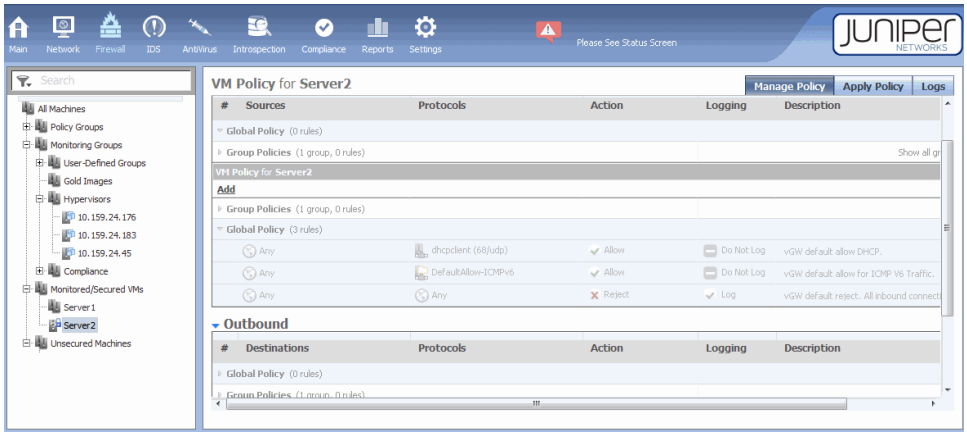
- The Firewall Module and the VM Tree on page 11
- Overview of the Firewall Policy Model on page 12
- Global Policy, Group Policy, and Individual VM Policy Tiers on page 13
- Firewall Policy Structure and Policy Rules Precedence on page 16
- Viewing the Complete Policy Rule Base for a VM on page 18
- The Manage Policy Tab on page 18
- The Apply Policy Tab on page 22
- The Logs Tab on page 23

The Firewall Module and the VM Tree

The Firewall module of the vGW Security Design VM allows you to define, apply, and monitor security policies. To change the data displayed on a Firewall module page, select all, one, or more than one VM in the VM tree. If you select one or more VMs, but not all, information pertaining to only the selected VMs is displayed. Figure 9 on page 12 shows information for a single VM.

Copyright © 2015, Juniper Networks, Inc.

Figure 9: Firewall Module Policy for a Single VM



Overview of the Firewall Policy Model

Security administrators of virtualized data centers invest a great deal of time and effort in planning their virtual infrastructures and building them out into group structures and categories to segment their VMs appropriately. The firewall policy model that they use to secure their virtualized infrastructure must be designed to accommodate the complexities that are intrinsic to the data center. Defining policy rules and building a firewall inside the middle of the data center differs in fundamental ways from building a perimeter firewall. Additionally, security for the virtualized data center infrastructure includes many challenges not the least of which is management of firewall policies for a large number of VMs.

The vGW Series Firewall policy used to secure the virtualized data center is modeled on the data center infrastructure overall, and it is purpose-built to meet its requirements.

- It entails group policy constructs to address group structures.
- It provides a means of simplifying the daunting task of creating policies for a large and increasing number of individual VMs.

  You can create reusable policies to apply across all VMs and groups of VMs, and you can define policy rules for individual VMs.
- It allows for flexible nesting to let you define policy rule precedence within these structures as they apply to an individual VM. You can change the order of rules within global, group, or individual sets of rules to control the effect of the policy.
- It addresses the need to build flows between different systems with greater granularity than a perimeter firewall design would entail.

Ultimately every VM has its own complete firewall policy, which is composed of some or all of these parts:

- Rules that apply to all VMs in your environment. Every VM policy contains them (Global Policy rules).
- Rules that apply to the individual VM *and* others like it, if a VM belongs to a group (Group Policy rules).

Copyright © 2015, Juniper Networks, Inc.

- Rules that apply only to that VM, if any are required (individual VM Policy rules).

  If a VM contains multiple vNICs, you can define separate policy rules for individual vNICs. These policy configurations show up in the VM rules section. See *Configuring the vGW Series Policy per vNIC Feature*.

The combination of these parts gives a VM a unique firewall rule base.

Global Policy, Group Policy, and Individual VM Policy Tiers

As with many firewall designs, the vGW Series firewall policy rules are applied in a top-down fashion. To ease management of a large number of VMs and to give you control over when rules are applied, the vGW Series firewall policy allows you to define policy at three tiers: the Global Policy tier, the Group Policy tier, and the VM Policy tier. You create a Global Policy and one or more Group Policy rule sets separately. vGW Series nests them appropriately for the individual VM when you create its policy. You can move policy rules within a tier to change precedence, controlling the order in which rules are executed.

At first glance the vGW Series firewall policy nesting model might seem complex, but its simplicity and usefulness become evident as you become familiar with the symmetry at the Global Policy and Group Policy tiers and the precedence relationship within a tier and among the tiers. The Global Policy tier has high-level and low-level sections that bound the policy; the Group Policy tier is nested within the Global Policy tier and it too has high-level and low-level sections. Individual VM Policy rules are nested at the center of a VM's policy between the Group Policy high-level and low-level sections.

Although a VM policy could contain policy rules at all three tiers, it is not necessarily the case. The following sections cover each of the policy tiers in particular, but to gain an overall sense of how they can be combined to create a policy consider the following:

Ultimately every VM has its own complete firewall policy, which is composed of some or all of these parts:

- Rules that apply to all VMs in your environment. Every VM policy contains them (Global Policy rules).
- Rules that apply to the individual VM *and* others like it, if a VM belongs to a group (Group Policy rules).
- Rules that apply only to that VM, if any are required (individual VM Policy rules).

  If a VM contains multiple vNICs, you can define separate policy rules for individual vNICs. These policy configurations show up in the VM rules section. See *Configuring the vGW Series Policy per vNIC Feature*.

Global Policy and Group Policy rule sets contain Inbound and Outbound parts.

Global Policy

You define a reusable Global Policy whose rules apply to every VM in your environment once—it is *global*. In that it is included in every VM's policy, the Global Policy is very powerful.

NOTE: **Although it is possible to delete all rules from the Global Policy, the concept of the Global Policy as applied before any other rules in the policy remains enforced. If you deleted all global rules, an empty Global Policy would be applied to the VM.**

Not to diminish their usefulness, you should take care in creating rules at the Global Policy level for the very fact that they are inherited by everyone.

Both the Inbound and Outbound parts of a firewall policy contain Global Policy sections. As is the case with many firewall configurations, by default the Global policy is restrictive. It is configured to allow inbound DHCP traffic and then to reject all other inbound traffic.

You can think of the Global Policy as a template or a container for the other nested parts that will compose the entire firewall policy for any VM, keeping in mind that the Global Policy itself consists of rules.

For both the Inbound and Outbound parts of a firewall policy, the Global Policy is segmented into the following two sections:

- High-level Global Policy rules

  These rules are positioned at the top of each part of a firewall policy. They are always applied to every VM first, whether that VM belongs to a group or is an individual VM. You use high-level Global Policy rules to enforce policy that cannot be overridden by any individual VM Policy rule.

  For example, in addition to enforcing corporate policy, you might use high-level Global Policy rules to prevent outbreaks and protect against vulnerabilities. You might add a Global Policy rule to block access to a vulnerable service until it is updated with all of the required patches.

- Low-level Global Policy rules

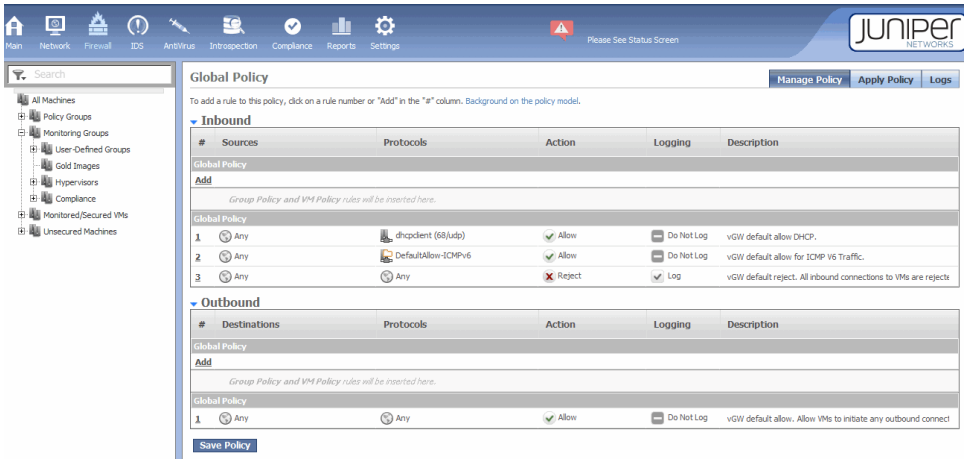
  These rules are positioned at the bottom of each part of a firewall policy. In any overall individual VM's firewall policy, they are applied last. They are applied to every VM. For example, for the Inbound part of a Global Policy, if an incoming connection is processed according to the appropriate firewall policy and it does not match any of the preceding rules, it falls through to the Inbound low-level Global Policy rules. Low-level Global policy rules are typically used as clean-up rules. By default, the Inbound low-level Global Policy rule rejects all connection attempts. It is defined as any-any-reject.

Between the high-level and low-level sets of Global Policy rules is a placeholder that allows for nesting of Group Policy rule sets and individual VM Policy rules.

To create a Global Policy, you select **GLOBAL POLICY** under Policy Groups in the VM tree. The page shown in Figure 10 on page 15 is displayed.

 Copyright © 2015, Juniper Networks, Inc.

Figure 10: Global Policy



Group Policy

Most of the daily policy management that security administrators of virtualized environments carry out is at the group level. Most likely you have structured your environment along lines of groups of VM with similar characteristics and you want to apply a similar policy to VMs that are members of a group.

NOTE: **In the nested model, a VM might belong to a Policy Group and inherit the Group Policy rules defined for that group, but it also might have its own individual VM Policy rules that contribute to its overall firewall policy rule base.**

For example, you might organize VMs into functional groups such as Web servers and database servers, and you might want to apply a different set of policy rules to each group. In your environment, you might create different groups for MS Windows systems versus Linux systems. To apply the appropriate security, you could define a different Group Policy for each of them.

The Group Policy concept allows you to define policy rules that are relevant to the VMs that comprise the group. As new VMs are created and added to a Policy Group, the Group Policy associated with the group is applied to them.

A VM might belong to multiple Policy Groups. For example, a VM might be a Windows VM and belong to the Windows group, but it also might be used as a Web server and belong to the Web servers group. In this case, the VM gets the Group Policy rules for both groups.

Individual VM Policy Rules

At the center of the entire firewall policy for an individual VM are any particular VM Policy rules that you define for that VM. Until this point, the firewall policy for an individual VM is composed of reusable parts—the Global Policy and, if the VM belongs to any Policy Groups, Group Policy rules.

Copyright © 2015, Juniper Networks, Inc.

You can apply individual VM Policy rules to a VM policy for particular purposes that distinguish that VM's policy from others. For example, you might want RADIUS access to a VM that is not applied at the Global Policy or Group Policy levels. To accomplish that, in the VM's firewall policy, you would define an Inbound VM Policy rule that allowed RADIUS access to the VM.

Default Policy

A newly created VM that does not have individual policy rules or group policy rules associated with it is automatically assigned the Default Policy. Also, when the policy for a VM includes one or more VM Policy rules but it does not include Group Policy rules, the VM inherits the Default Policy rules, in addition to the individual ones. Later if it becomes a member of a group, then it inherits that group's Group Policy rules, and the Default Policy rules no longer apply.

By default, the Default Policy does not contain any policy rules. It is assumed that you will define the policy that you want to use as the default.

Quarantine Policy

When a VM is infected by a virus and the scanning configuration specifies "Quarantine the VM", the VM is put in the Quarantine policy group. The Quarantine Policy that you define is applied to all VMs in the Quarantine policy group. When you remove the VM from the group, the Quarantine policy is removed.

To remove the VM from the Quarantine policy group, use the Main module Quarantine tab. Select the VM, and click **Un-quarantine**.

For details on how the parts of the quarantine process work together for a quarantined VM, see "Understanding Quarantined VMs and How to Manage Them" on page 152.

Firewall Policy Structure and Policy Rules Precedence

The vGW Series Firewall policy model is premised on a pre-post concept that allows you to manage rules execution precedence.

Consider the nested structure of a firewall policy. To summarize the order, a firewall policy has inbound and outbound sections. The Inbound section contains the high-level Global Policy rules followed by, the Group Policy rules, then the individual VM Policy rules, and finally the default Global Policy rules. The default Global Policy rules consist of a rule to allow DHCP traffic, a rule to allow certain types of ICPMv6 traffic, and, at the bottom, a rule to reject all other inbound traffic. The outbound section contains the same parts in the same order, only its Global Policy section contains a single rule that allows VMs to initiate outbound connections.

high-level Global Policy— At the top of the Inbound section is the high-level Global Policy tier, containing any global policies that you add.

high-level Group Policy—Beneath it is the high-level Group Policy section containing any of Policy Groups rule sets that apply to the individual VM that you want executed *before* the individual VM Policy rules.

 Copyright © 2015, Juniper Networks, Inc.

VM Policy—Beneath it is the high-level VM Policy section containing any individual rules that you define for the VM whose policy you are creating.

low-level Group Policy—Beneath it is the low-level Group Policy section containing any group rule sets for the VM that you want to be executed *after* its individual ones.

Default Global Policy—The default Global Policy rules consist of a rule to allow DHCP traffic, a rule to allow certain types of ICPMv6 traffic, and, at the bottom, a rule to reject all other inbound traffic.

It is this structure that allows you to manipulate the order in which rules are executed for the individual VM firewall policy. The vGW Series Policy model affords you extensive, flexible control over the order in which rules are executed. You can move rules up and down within their sets; you can move rules from a low-level section of one tier to that tier's high-level section or the opposite, and you can reorganize individual VM Policy rules.

Rules are executed in a top-down fashion:

- High-level Global Policy rules are always executed first, and that cannot be changed.

  However, you can manage the order in which Global Policy rules are executed by moving them up and down in the set.

- High-level Group Policy rules are executed next. They are always executed before individual VM Policy rules, but you can also change the order in which they are executed by moving them up and down within the set.
- Individual VM Policy rules are executed next, and you can change their order to control when they are executed.
- Low-level Group Policy rules are always executed after the individual VM Policy rules.

  By placing some of the Group Policy's rules in its low-level section, you are able to specify that in most cases you want these rules applied to all VMs that belong to the Policy Group *after* the individual VM Policy rules are executed. You will allow VM Policy rules for individual VMs to take precedence over these Group Policy rules.

- Finally, low-level Global Policy rules are executed for every VM.

For example:

- If you move a rule *up* from its low-level Group Policy section to its high-level counterpart, that rule is executed *before* any individual VM Policy rule, and it *cannot* be overridden by a VM Policy rule. Previously, when it resided in the low-level Group Policy section, a VM Policy rule could override it.
- If you move a rule *down* from its high-level Group Policy section to its low-level counterpart, that rule is executed *after* any individual VM Policy rule, and it *can* be overridden by a VM Policy rule. Previously, when it resided in the high-level Group Policy section, a VM Policy rule could not override it.

When you nest rules for a VM's firewall policy, take into account precedence among the various levels of the policy. For example, consider a policy for a VM whose inbound low-level Group Policy section includes a rule that allows management access to the

Copyright © 2015, Juniper Networks, Inc.

VM. Suppose that as the data center administrator you will always want management access to the VM. However, you understand that another administrator could create a firewall policy intended for an individual VM that is a member of the Windows VMs group as part of the group policy. That administrator could define a VM Policy rule for the individual VM that would reject management access to the VM, effectively denying you access. Because the Group Policy rule allowing access is in the low-level section of the Group Policy rule set, the individual VM Policy rule would override it.

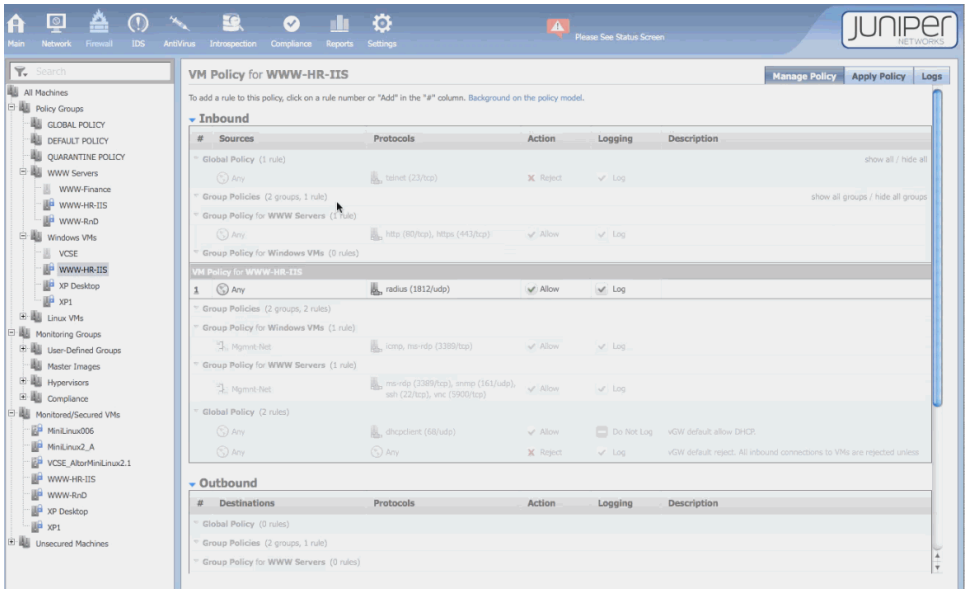
To ensure that you always have management access, you could affect the precedence in the policy for any VM that belongs to that group by moving the rule that allows management access up from the low-level Group Policy section to the high-level Group Policy section. To do so, click the rule number in the low-level Group Policy and select **Move Rule Up** from the list.

Viewing the Complete Policy Rule Base for a VM

Each VM protected by a vGW firewall policy can be thought of as having its own firewall policy. The resulting full policy for a VM always includes a Global Policy, Group Policies if the VM belongs to Policy Groups, and individual VM Policy rules that are specific to it.

After you have created a firewall policy for a VM or you want to understand its policy, you can expand it to see its entire rule base. To do this, select the Firewall module. In the VM tree, select the VM. On the upper-right side of the VM Policy page, click **show-all** . See Figure 11 on page 18.

Figure 11: VM Policy Expanded Rule Base



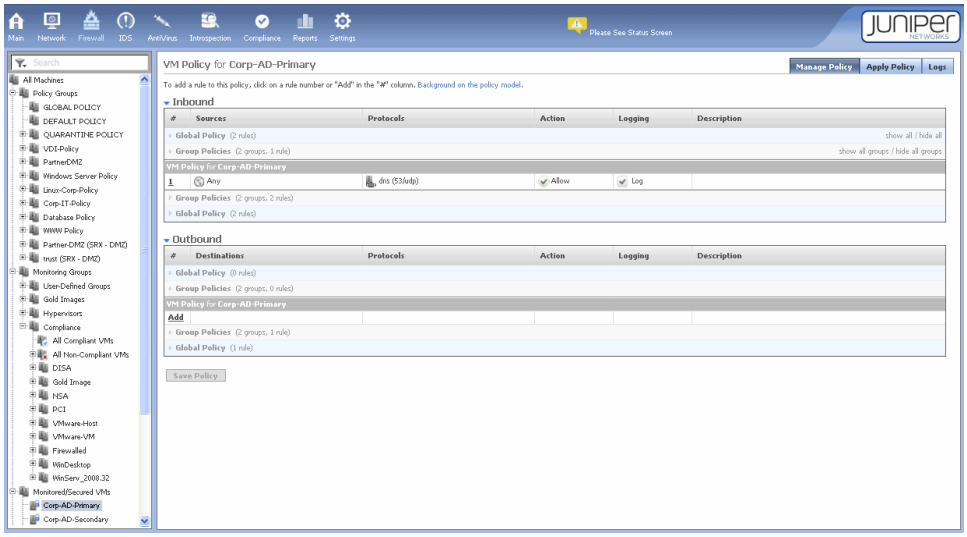
The Manage Policy Tab

The Manage Policy tab allows you to define and edit security policies. The Manage Policy page shows the policy configured for the group of VMs or the VM that is selected in the VM tree. To change the data displayed on the Manage Policy page, select a different

Copyright © 2015, Juniper Networks, Inc.

object in the VM tree. You can select all machines, a group, or an individual VM. Figure 12 on page 19 shows the policy for the Corp-AD-Primary VM.

Figure 12: Firewall Module Manage Policy Page



This section contains the following parts:

- Policy Per vNIC and Dual Stack on page 19
- Creating a Policy Rule on page 19

Policy Per vNIC and Dual Stack

A single VM may have multiple vNICs attached to it. In the case of a dual stack, a VM would have a vNIC with an IPv4 address and an IPv6 address bound to it.

vGW Series provides a feature called Policy per vNIC that allows you to define separate policies for individual vNICs attached to the same VM. You can configure separate policies for individual vNICs, separate policies for some of them while leaving others unsecured, or you can use the same policy for all of them.

Using the Policy per vNIC feature, you can handily apply different policy rules to vNICs passing IPv4 traffic from those used for IPv6 traffic even when the vNICs are attached to the same VM. To apply the rule to all traffic of a type, you could use the predefined terms **Any-IPv4** and **Any-IPv6**.

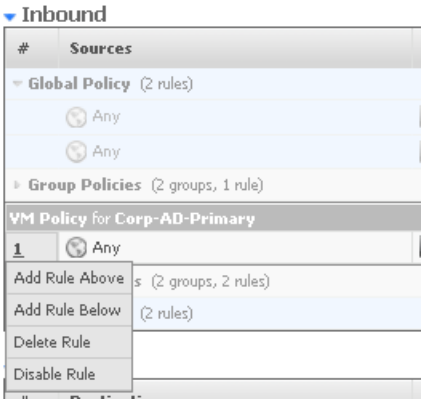
Creating a Policy Rule

To create a policy rule:

1. Click a rule number in the rule numbers (#) column.
2. Select **Add Rule Above** or **Add Rule Below**. See Figure 13 on page 20.

Copyright © 2015, Juniper Networks, Inc.

Figure 13: Adding a Rule



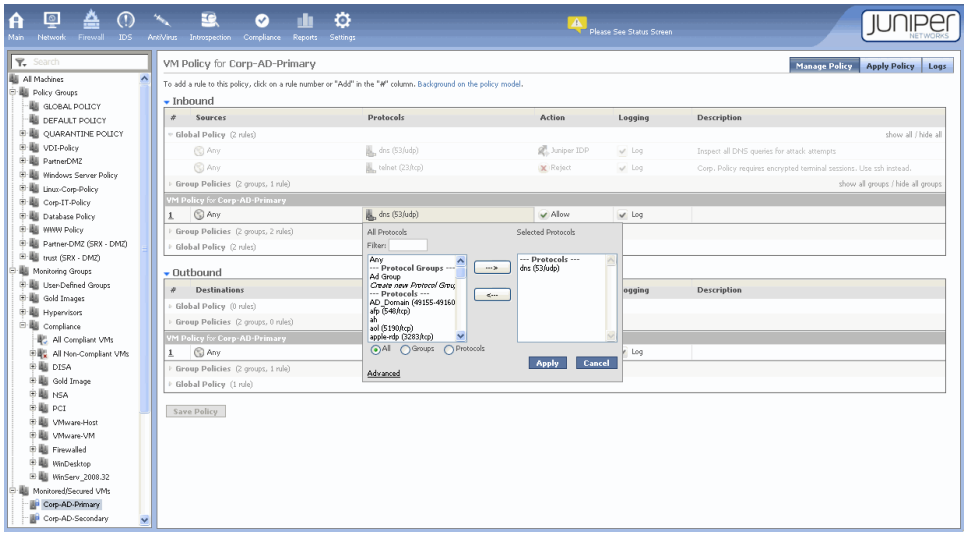
NOTE: **Rules are applied in order of execution from top to bottom.**

3. Configure policy settings by clicking the table cells and editing the information using the dialog box.

   For example, to specify a protocol for the rule, click the default value **Any**, which displays a dialog box. To quickly make selections, type the first letter of the item that you want to select in the filter field. See Figure 14 on page 20.

   Typing the letter **t** in the All Protocols dialog box scrolls to the telnet selection in the list.

Figure 14: Using the Dialog Box Filter to Add Terms for policy rules



To immediately select an item, type directly into the Filter box.

Copyright © 2015, Juniper Networks, Inc.

To define a policy that contains all protocols except for a few:

1. Click **Advanced** at the bottom of the dialog box.
2. Click **Negate this selection**.

   As a result, "All protocols except" is displayed at the top of the Selected Protocols list.
3. For each protocol or protocol group that you want to exclude from the policy rule, select the object and click the right arrow to move it to the list.
4. Click **Apply**, when you are finished.
5. When you have finished entering or editing all policy settings, click **Save** to save your changes in the vGW Security Design VM database.

WARNING: **For new policy rules to take effect, you must apply the policy changes using the Apply Policy tab. You can apply rules immediately or during maintenance.**

To delete or disable/deactivate an existing rule, click the rule number and choose the appropriate option. Disabled rules appear dimmed and are shown with a strike-through mark.

Table 4 on page 21 describes the policy configuration settings.

Table 4: Firewall Policy Configuration Settings

Field	Function
Sources	Define the object from which the connection originates.
Protocols	Define which protocols are used in the rule. You can also dynamically create a new protocol or protocol group by selecting the appropriate option.
Action	Allow the connection, drop the connection (silent drop), or reject the connection (drop traffic and send source a notification). In addition, you can redirect or duplicate packets to third-party devices using Settings > Security Settings > Global > External Inspection Devices. See *Configuring Global Settings Using the vGW Series Settings Module (VMware)*.
Logging	Log the connection matching the rule, skip logging for this connection, or send an alert when this connection matches the rule. The Alert option directs the vGW Series to send e-mail messages or SNMP traps. See "Alerts" on page 80.
Description	Enter a description for the policy.

Copyright © 2015, Juniper Networks, Inc.

The Apply Policy Tab

The Apply Policy tab allows you to push security policies out to the vGW Security VM firewall to protect the VMs in your infrastructure. When you create or modify a policy, it is not applied to the VM automatically. For new policy rules to take effect, you must apply the policy changes using the Apply Policy tab. You can apply rules immediately or during maintenance.

You use the VM tree on the left side of the Apply Policy page to select the VMs to apply policies to.

Reflecting the hierarchy in which you create a VM policy, the Apply Policy table shows:

- That the VM has a Global Policy, its Group Policies, if it belongs to a group, and any individual policies configured specifically for it.

  NOTE: **If there are no Group or individual policy rules for a VM, the Global Policy is applied.**

- If a VM has multiple vNICs, whether Policy per vNIC is applied to it.
- The vGW Security VM that protects the VM.
- The date that the policy was installed.

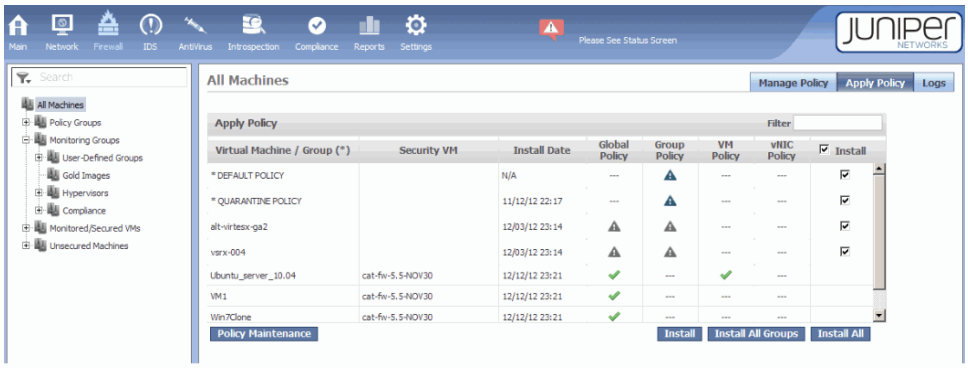
To install a policy on one or more selected VMs:

1. Select the **Install** check box at the right of the title bar.
2. Select the check box in the Install column at the right of the VM's row.
3. Click **Install** at the bottom of the page.

   To install policies for all VMs, click the **Install** check box at the top of the column, then click**Install All**. To install policies for all Groups, click **Install All Groups**.

Figure 15 on page 22 shows the Apply Policy page.

Figure 15: Firewall Apply Policy Page



Copyright © 2015, Juniper Networks, Inc.

See Table 5 on page 23 for a list of icons displayed for VMs on the Apply Policy page.

Table 5: Firewall Policy Icons

Icon	Indicates that
	The policy is current and no further actions are required.
	The VM is in a policy group, but it cannot retrieve policies because it is not protected by a vGW Security VM firewall. This usually indicates an error condition that you should investigate.
---	The policy type does not exist for the VM. For example, an individual VM policy for that VM is not configured. You are not required to build individual VM policies for each VM.
	The policy has been modified, and it needs to be deployed for the VM.
	An error condition exists that prevents installation of the policy. When a policy distribution problem exists but the old policy works properly, a check mark icon might be displayed.

TIP: **Place the pointer over a policy status icon to display a tool tip that describes the icon.**

When you are ready to implement a policy, click either **install** or **install all** to push the policy out to the firewall. This action causes the policy to be deployed on the selected VMs or the vNICs of the VMs, if the Policy per vNIC feature is used.

NOTE: **When you attempt to apply a policy to a vNIC that is not secured and that belongs to a protected VM, the policy is not applied. The following message is displayed:**

"Policy was compiled and saved. This VM is currently not associated with a firewall, so the policy is not being immediately loaded on a firewall. This could be because the VMs migrated to an unprotected host or are powered off. Once the VM will be associated to a firewall, the corresponding saved policy will be enforced."

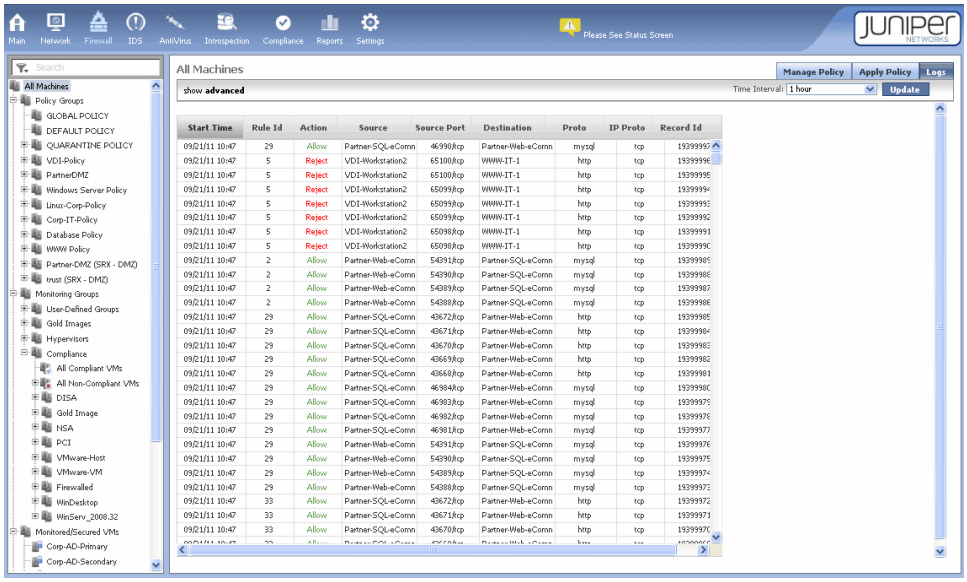
The Logs Tab

You can define policy rules to specify Log, Don't Log, and Alert notification options. When you select **Log** or **Alert** for a rule, traffic that matches that rule is logged.
Figure 16 on page 24 shows the Logs tab.

For the Logs tab, you can use an advanced option that includes a mark verified VMs setting. vGW Series uses the unique VMware ID/UUID in addition to an IP address to validate that connections are coming from the identified server. This feature protects the network from issues such as IP spoofing and DHCP changes. VMs for which this extra validation is allowed are flagged with an asterisk (*). You can use the mark verified VMs setting to display or hide the icon. Click **Auto-refresh** to refresh the log displayed automatically every 60 seconds.

The log entries show both IPv4 and IPv6 addresses.

Figure 16: Firewall Module Logs Tab



You can use filters to refine the display of log entries. To display only those logs related to a specific VM, select the VM in the VM tree pane.

Related Documentation

- *Understanding the vGW Series Policy per vNIC Feature*
- *Understanding the vGW Security Design VM*
- *Understanding the vGW Security Design VM Taskbar*
- *About the vGW Security Design VM Tree*
- Understanding the vGW Series Network Module on page 3
- *Understanding vGW Series*

Understanding How vGW Series Handles ICMPv6 Protocol Traffic

This topic covers the Internet Control Message Protocol version 6 (ICMPv6) which is integral to IPv6 and fundamental to the proper functioning of IPv6 networks.

It describes the vGW Series default firewall policy protocol group for handling ICMPv6 traffic.

Copyright © 2015, Juniper Networks, Inc.

WARNING: By default vGW Series allows inbound and outbound ICMPv6 traffic. Juniper Networks strongly recommends that you not override this default policy because of the important role that ICMPv6 plays in establishing and maintaining communication in IPv6 networks.

- About ICMPv6 on page 25
- Filtering ICMPv6 Packets on page 25
- Default Policy Group for Allowing Inbound ICMPv6 Packets on page 26

About ICMPv6

ICMPv6 consists of a large number of messages with diverse functions which, like ICMP messages for IPv4 networks, could be categorized broadly as error and information messages.

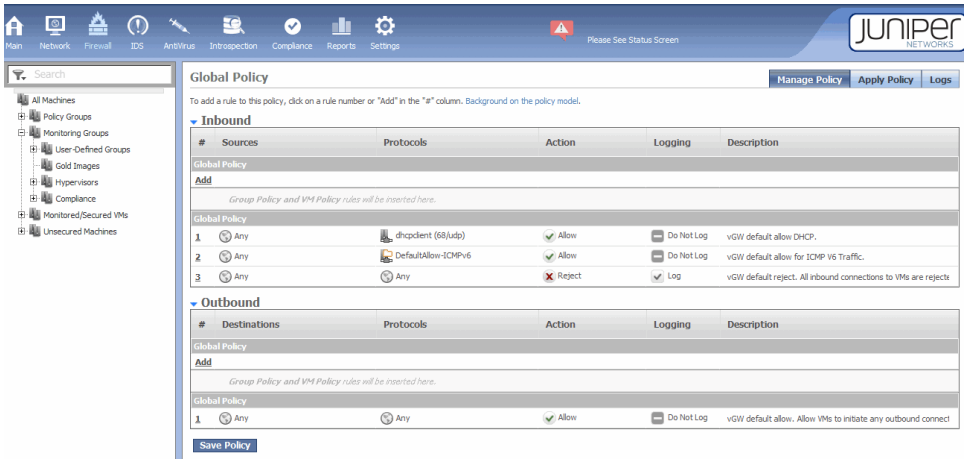
ICMP for IPv4 is an auxiliary protocol not necessarily required for IPv4 proper functioning. By contrast, ICMPv6 is an essential component in the establishment and maintenance of IPv6 communications. Among the messages it includes are those for address assignment, address resolution, and multicast group management. ICMPv6 error messages and information messages are transported by IPv6 packets in which the IPv6 Next Header value for ICMPv6 is set to 58.

Filtering ICMPv6 Packets

In IPv4 networks, it is common practice for firewalls to drop ICMP Echo Request messages to protect against scanning attacks and to minimize the risk of denial of service attacks. Port scanning in IPv6 networks is less severe, so it is not necessary to filter IPv6 Echo Requests. In practice, it is important to avoid aggressive filtering of ICMPv6 packets. Because they are fundamental to the proper functioning of IPv6 networks and tunneling, it is essential that ICMPv6 connectivity messages are allowed to pass through the firewall.

vGW Series establishes a default protocol group called DefaultAllow-ICMPv6 that allows access to traffic from a comprehensive set of ICMPv6 protocols. A default rule for the DefaultAllow-ICMPv6 protocol is created that is applied to the inbound Global policy rule set to allow this inbound traffic. See Figure 17 on page 26.

Figure 17: Default Global Policy Showing Default ICMPv6 Allow Group



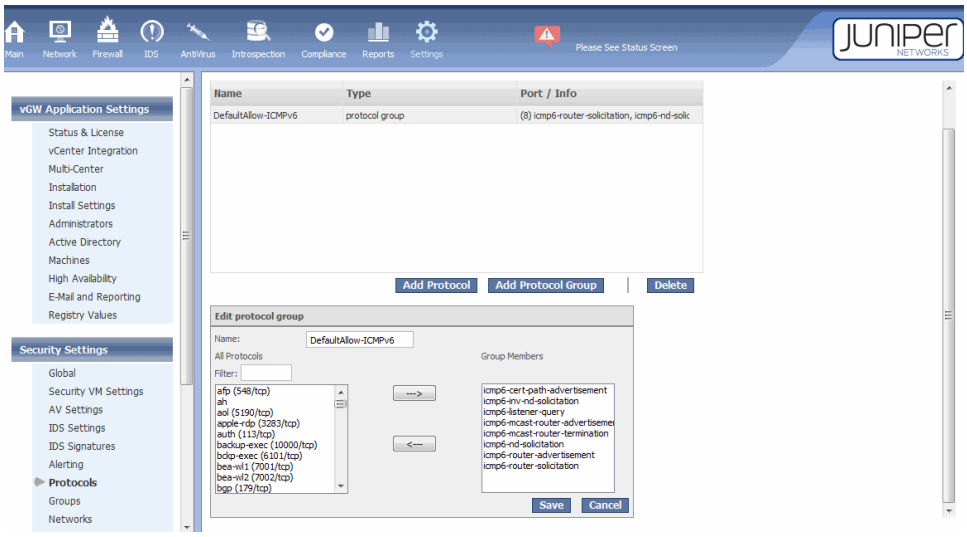
Default Policy Group for Allowing Inbound ICMPv6 Packets

vGW Series provides the predefined DefaultAllow-ICMPv6 protocol group that allows inbound ICMPv6 traffic for all types of packets included in the group. Because ICMPv6 is critical to proper IPv6 functioning, it is important that you allow this traffic. However, if for some reason you wish to block traffic from one or more ICPMv6 protocols that are members of the default protocol group, you can edit the list to exclude them from the *allow* condition and filter the traffic. See "Editing the Default ICMPv6 Protocols Group Members" on page 27.

Viewing the Default ICMPv6 Protocols Group Members

You can view the list of ICMPv6 protocols that comprise the DefaultAllow-ICMPv6 protocol group on the Settings module Security Settings > Protocols page. See Figure 18 on page 26.

Figure 18: Protocols Settings ICMPv6 Default Protocol Group



Copyright © 2015, Juniper Networks, Inc.

To view the list:

1. Beside **Protocols**, select **Groups**.
2. Click **DefaultAllow-ICMPv6**.

   The column on the right side of the Edit protocol group pane shows the group members:

   - icmp6-listener-query

     130. Multicast Listener Query (RFC 2710)
   - icmp6-router-solicitation

     133. Router Solicitation (RFC 4861)
   - icmp6-router-advertisement

     134. Router Advertisement (RFC 2461)
   - icmp6-nd-solicitation

     135. Neighbor Discovery Solicitation (RFC 4861)
   - icmp6-inv-nd-solicitation

     141. Inverse Neighbor Discovery Solicitation Message (RFC 3122)
   - icmp6-cert-path-advertisement

     149. Certification Path Advertisement Message (RFC 3971)
   - icmp6-mcast-router-advertisement

     151. Multicast Router Advertisement (RFC 4286)
   - icmp6-mcast-router-termination

     153. Multicast Router Termination (RFC 4286)

Editing the Default ICMPv6 Protocols Group Members

If you must block traffic on any of the ICMPv6 protocols in the vGW DefaultAllow-ICMPv6 protocol group, you can edit the group from Settings module Security Settings > Protocol page.

To edit the list from the Settings module Security Settings > Protocol page:

1. Beside **Protocols**, select **Groups**.
2. Click **DefaultAllow-ICMPv6**.

   The column on the right side of the Edit protocol group pane shows the group members:

   - icmp6-cert-path-advertisement
   - icmp6-inv-nd-solicitation
   - icmp6-listener-query
   - icmp6-mcast-router-advertisement
   - icmp6-mcast-router-termination

Copyright © 2015, Juniper Networks, Inc.

- icmp6-nd-solicitation
- icmp6-router-advertisement
- icmp6-router-solicitation

3. Select the ICMPv6 protocol that you want to remove from the list, thereby blocking its packets, and click the left facing arrow.

   Repeat this process for each protocol that you want to remove from the list.

4. Click **Save**.

Related Documentation

- Understanding the vGW Series Firewall Module on page 11
- Understanding vGW Series Predefined Firewall Policy for Its Components on page 38
- *Understanding vGW Series IPv6 Support*
- *Understanding vGW Series*
- *Understanding the vGW Series Settings Module*

Understanding Predefined Objects for vGW Series Firewall Policy Terms

This topic focuses primarily on the vGW Series predefined objects that you can use for source and destination terms in firewall policy rules. It summarizes the various ways in which you can specify addresses for these terms.

- Defining and Selecting Source and Destination Terms for Policy Rules on page 28
- Predefined Global IP Address Objects on page 29
- Predefined Network Objects on page 29

Defining and Selecting Source and Destination Terms for Policy Rules

To create firewall policies, you specify rules. You add inbound and outbound rules to a policy to specify the source and destination of traffic. You select a value for the source or the destination of a term from the list of existing objects that is displayed when you right-click the rule numbers column in the Inbound (Sources) and Outbound (Destinations) parts of a policy.

vGW Series provides the following ways in which you can define the addresses for a rule's source or destination terms:

- You can define these addresses dynamically as you create the rule. You can create groups or machines and then use them in the rule.

  As a convenience, the vGW Security Design VM makes the configuration panes that you use for this purpose available from the Manage Policy page of the Firewall module that you use to define the policy. They are the same panes that you use to create the objects from other parts of the vGW Security Design VM.

- You can select a network or a machine that you have already defined.

Copyright © 2015, Juniper Networks, Inc.

- You can select any of the predefined objects that vGW Series provides. The following sections cover these objects.

Predefined Global IP Address Objects

vGW Series Release 5.5 introduces support for IPv6, including configuration of policies on IPv6 traffic. vGW Series provides the following predefined objects that allow you to refer to IP addresses collectively by type–whether IPv4 addresses or IPv6 addresses–in a policy rule's source and destination terms:

Any—Matches any IPv4 and IPv6 address.

Any-IPv4—Matches any IPv4 address.

Any-IPv6—Matches any IPv6 address.

In releases earlier than version 5.5–releases before vGW Series supported IPv6– the term Any referred to any IPv4 address. For environments in which not all vGW Series components are at version 5.5 or later, the term Any also refers to any IPv4 address. It reverts back to the meaning it had in environments that support only IPv4 traffic. For more information about how Any is interpreted in mixed vGW Series components environments, see *IPv6 Support in Homogeneous and Heterogeneous vGW Series Environments*.

WARNING: **All vGW Series components must be at version 5.5 or later for you to be able to create policies on IPv6 traffic.**

Predefined Network Objects

vGW Series provides predefined network objects for well-known IP address ranges and prefixes that you can use in policy rule terms for either source or destination addresses. It also provides network objects for other IPv6 and IPv4 addresses. This section covers both groups.

NOTE: **Prior to vGW Series Release 5.5, you used the Settings module Security Settings > Global Settings Rules pane to control broadcast and multicast settings. As of Release 5.5, you can no longer set these parameters from the Global Settings Rules pane. Rather, you must use the corresponding network object in a policy rule to control the firewall behavior.**

Copyright © 2015, Juniper Networks, Inc.

Predefined Network Objects for Well Known IP Addresses

vGW Series provides the following predefined network objects that you can use in policy rule terms as either source or destination addresses:

- Link Local Addresses (**fe80::/10**)

  IPv6 link-local addresses are defined in section 2.5.6 of the IEFT RFC 4291 standard as having a 10-bit prefix of **fe80** followed by 54 zero bits and a 64-bit interface ID.

  A link-local address is an IP address that is intended for communications within the link, or segment, of a local network or a point-to-point connection that a host is connected to. These addresses are useful for establishing communication across a link in the absence of a globally routable prefix or for intentionally limiting the scope of traffic that should not be routed. IPv6 link-local addresses, therefore, can be used only within the context of a single Layer 2 domain. Packets sourced from or destined to a link-local address are not forwarded out of the Layer 2 domain by routers.

- IPv4 Mapped Addresses (**::ffff:0.0.0.0 – ::ffff:255.255.255.255**)

  The IEFT RFC 6052 standard *IPv6 Addressing of IPv4/IPv6 Translators* covers the algorithmic translation of an IPv6 address to a corresponding IPv4 address, and vice versa, using statically configured information. Algorithmic translation is used in IPv4/IPv6 translators and other types of proxies and gateways that are used in IPv4/IPv6 scenarios, such as DNS.

  NOTE: **vGW Series accepts both IPv4 and IPv6 address formats and displays the addresses as you enter them.**

- Well Known Prefix for IPv4 (**64:ff9b::/96**)

  The IEFT RFC 6052 standard *IPv6 Addressing of IPv4/IPv6 Translators* covers the Well Known Prefix **64:ff9b::/96** that is used in an algorithmic mapping between IPv4 to IPv6 addresses. It is defined out of the **0000::/8** address block.

- IPv4 Local Broadcast (**255.255.255.255**)

  A special definition exists for the IP broadcast address **255.255.255.255**. It is the broadcast address of the zero network or **0.0.0.0**, which in IP standards implies the local network. Transmission to this address is never forwarded by the routers connecting the local network to other networks.

Additional IPv4 and IPv6 Predefined Network Objects

- Unspecified IPv4 (all zeros)

  In IPv4, an IP address of all zeroes (**0.0.0.0**) has a special meaning. It refers to the host itself. It is used when a device does not know its own address.

- Unspecified IPv6 (all zeros)

  The IPv6 unicast unspecified address is equivalent to the IPv4 unspecified address. The IPv6 unspecified address is **0:0:0:0:0:0:0:0:**, or a double colon (**::**). In IPv6, this

Copyright © 2015, Juniper Networks, Inc.

concept has been formalized. It is typically used in the source field of a datagram sent by a device seeking to have its IP address configured.

- Loopback IPv4 (**127.0.0.1**)

  The IEFT RFC 2606 standard officially reserved domain name for the IPv4 and IPv6 loopback network addresses is localhost.

  In IPv4, this network has the prefix **127.0/8**, as defined in the IEFT RFC 3330 standard. The most commonly used IP address on the loopback device is **127.0.0.1** for IPv4, although any address in the range **127.0.0.0** to **127.255.255.255** is mapped to it.

- Loopback IPv6 (**::1**)

  The IEFT RFC 2606 standard officially reserved domain name for the IPv4 and IPv6 loopback addresses is localhost. IPv6 designates only a single address for the IP loopback function, **::1**. The **::1/128** prefix is defined in the IEFT RFC 3513 standard.

- Multicast IPv4 (**224.0.0.0/4**)

  A multicast address is a logical identifier for a group of hosts in a network that are available to process datagrams or frames for a designated network service. IPv4 and IPv6 multicast addressing is used at Layer 3 (OSI) for IPv4 and IPv6.

  The Classless Interdomain Routing (CIDR) prefix of multicast addresses is **224.0.0.0/4**. The group includes the addresses from **224.0.0.0** to **239.255.255.255**. Address assignments from within this range are specified in the RFC 5771 standard.

- Multicast IPv6 (**ff00::/8**)

  Multicast addresses in IPv6 have the prefix **ff00::/8**. IPv6 multicast addresses are generally formed from 4-bit groups, illustrated as follows:

  - Prefix: The **prefix** holds the binary value **11111111** for any multicast address.
  - Flags: Currently, 3 of the 4 flag bits in the **flgs** field are defined. The left-most, most-significant flag bit is reserved for future use.
  - Scope: IPv6 multicast addresses specify their scope. The set of possible scopes is different. The 4-bit **sc**, or scope, field (bits 12 to 15) is used to indicate whether the address is valid and unique.
  - Group ID: The 112-bit **group ID** field identifies the service. For example, if **ff02::101** refers to all Network Time Protocol (NTP) servers on the local network segment, then **ff08::101** refers to all NTP servers in an organization's networks. The Group ID field may be further divided for special multicast address types.

Related Documentation

- Understanding the vGW Series Firewall Module on page 11
- Configuring vGW Series Firewall Policies on page 32
- *Understanding the vGW Series Policy per vNIC Feature*
- *Understanding vGW Series*

Configuring vGW Series Firewall Policies

This topic covers how to create a firewall policy for a VM composed of the corporate Global Policy, two Group Policies for the groups that the VM is a member of, and one VM Policy rule applicable to the individual VM.

It covers the preliminary tasks of defining the reusable Global Policy and a Group Policy for one of the groups that the VM is a member of.

Before you begin this procedure, read "Understanding the vGW Series Firewall Module" on page 11. The procedure for composing an overall policy for a VM includes these parts:

- Define a Global Policy. The Global Policy is a reusable policy that is inherited by firewall policies for all VMs. You need to define it only once.

  When you select the Firewall module and a VM in the VM tree to create a VM policy for it, the VM policy automatically inherits the Global Policy that you have created.

- Define Group Policies for the groups that the VM belongs to. You can define a Group Policy for a Policy Group any time after the Policy Group is created.

  If the individual VM belongs to a Policy Group, it automatically inherits the Group Policy defined for that Policy Group, if the Group Policy is already defined.

  When you select the Firewall module and a VM in the VM tree to create a VM Policy for it, the VM Policy contains the Group Policies that you created for any groups that the VM is a member of.

  After you define the Group Policy for a group, it is automatically used in the individual policies that you construct for all members of the group. VMs that are created later and added to the policy group, either manually or automatically, inherit the Group Policy rules for that group.

  NOTE: **To illustrate precedence setting, this example assumes that the Group Policy already exists. It shows how to modify it.**

- Define an individual VM Policy for the VM. At this point, you build the overall policy for the VM.

  The VM Policy for a VM is composed of the Global Policy, Group Policies for any groups that it belongs to, and any individual VM Policy rules that you want to apply to that VM in particular.

  When you select the Firewall module and a VM in the VM tree to create a VM Policy for it, the policy automatically inherits the Global Policy and the Group Policies for any groups that the VM is a member of. To complete the individual VM Policy, you add any VM Policy rules that you want to apply to that VM only. For example, you might need RADIUS access to a particular VM and not to others. You could apply a VM Policy rule to that VM's individual policy.

Copyright © 2015, Juniper Networks, Inc.

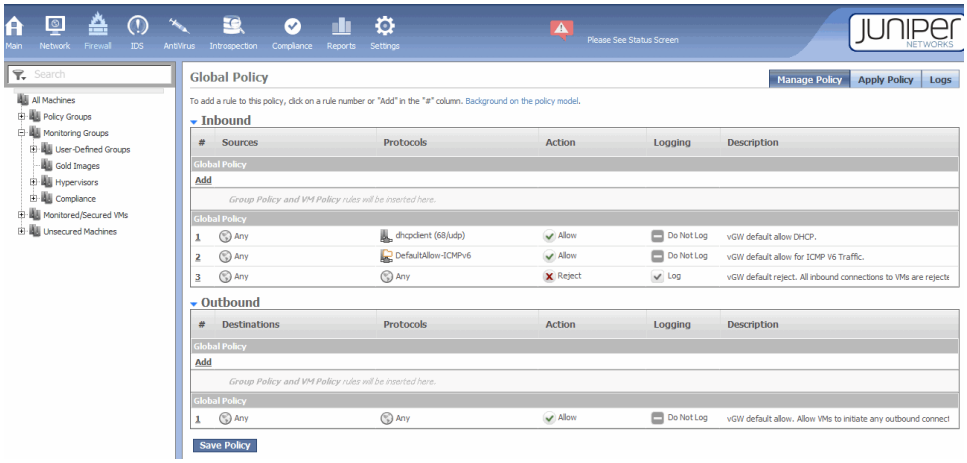
Create a reusable Global Policy to be used as part of the VM policies for all VMs in your environment.

NOTE: **This example focuses on defining an inbound policy only. The process of defining outbound policy mirrors it.**

1. Define a Global Policy. From the Firewall module, select **Global Policy** under the Policy Groups section in the VM Tree.

   The Global Policy page appears. It contains Inbound and Outbound sections. Each section contains a high-level Global Policy section and a low-level Global Policy section with a placeholder for Group Policy rules and individual VM Policy rules in the middle. Figure 19 on page 33 shows the Global Policy with its default policy rules.

Figure 19: Default Global Policy



2. Create an Inbound high-level Global Policy rule to prohibit use of Telnet.

   a. In the Inbound section, click **Add** in the # column under the first section labeled Global Policy to add a rule.

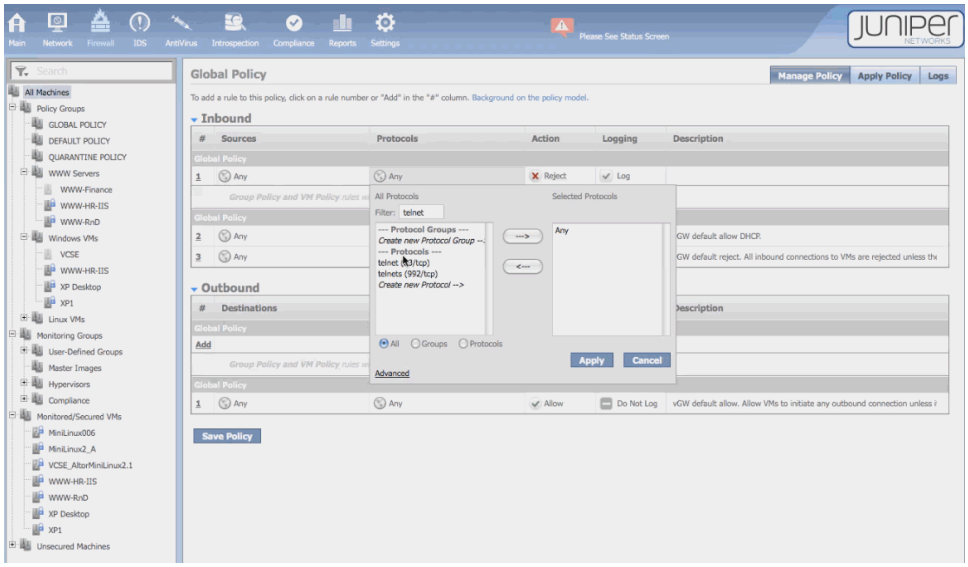
   b. For the Sources policy term, leave the default value Any unchanged.

      You want the rule to apply to all VMs.

   c. Click **Any** in the Protocols column, and enter **telnet** in the Filter box. The filter scrolls to **telnet**.

   d. Select **telnet**, and click the right arrow to move telnet from the All Protocols section to the Selected Protocols section. See Figure 20 on page 34.

Figure 20: Adding a Global Policy Rule to Reject Telnet Connection Attempts



e. Click **Allow** in the actions column and select **Reject** from the Action options list. You want to reject all inbound Telnet connections attempts for all VMs in your environment.

f. Leave the check mark default setting for Logging unchanged. Although they are rejected, you want to log any Telnet connection attempts.

3. Leave the low-level Global Policy rule unchanged.

   By default, the last rule serves as a "clean-up" rule that catches all inbound connection attempts to this VM that have fallen through the rest of the policy rule base. It rejects them, and it specifies that vGW Series should create a log entry for the event.

4. Click **Save Policy**.

Modify the Group Policy for the Window VMs Policy Group to control rule execution precedence.

This procedure allows you to modify an existing Group Policy to change rule execution precedence. You want to ensure that a rule currently positioned in the low-level Group Policy section is not overridden by a VM Policy rule that might be inserted above it when an individual VM policy that includes the Group Policy is created. You want that rule to be executed *before* any VM Policy rules. To achieve that result, move the rule up from the low-level Group Policy section to the high-level Group Policy section.

NOTE: **This example focuses on defining an Inbound policy only. An outbound policy definition process mirrors it.**

1. In the Policy Groups section of the VM tree, select **Windows VMs**.

Copyright © 2015, Juniper Networks, Inc.

Notice that the high-level and low-level Group Policy sections are nested within the high-level and low-level Global Policy sections.

indicates the placeholder for adding VM Policy rules at the center of the Group Policy section.

2. Move the network management rule from the low-level Group Policy section to the high-level Group Policy section so that any VM Policy rule for an individual VM Policy rule added later cannot override it. See .
3. Click **Save Policy**.

Create a VM Policy for an individual VM

This procedure covers how to create individual VM policy rules for the WWW-HR-IIS VM that inherits the Global Policy and the Group Policies for the groups that it is a member of. An individual VM can belong to more than one Policy Group. When that is the case, the VM inherits the Group Policies for all of the Policy Groups that it belongs to. In this example, the WWW-HS-IIS VM is a member of two Policy Groups: WWW Servers and Windows VM.

This example focuses on the Inbound section of the VM Policy.

1. To display the VM Policy for the WWW-HR-IIS VM, select **WWW-HR-IIS** in the Windows VMs under Policy Groups in the VM Tree.

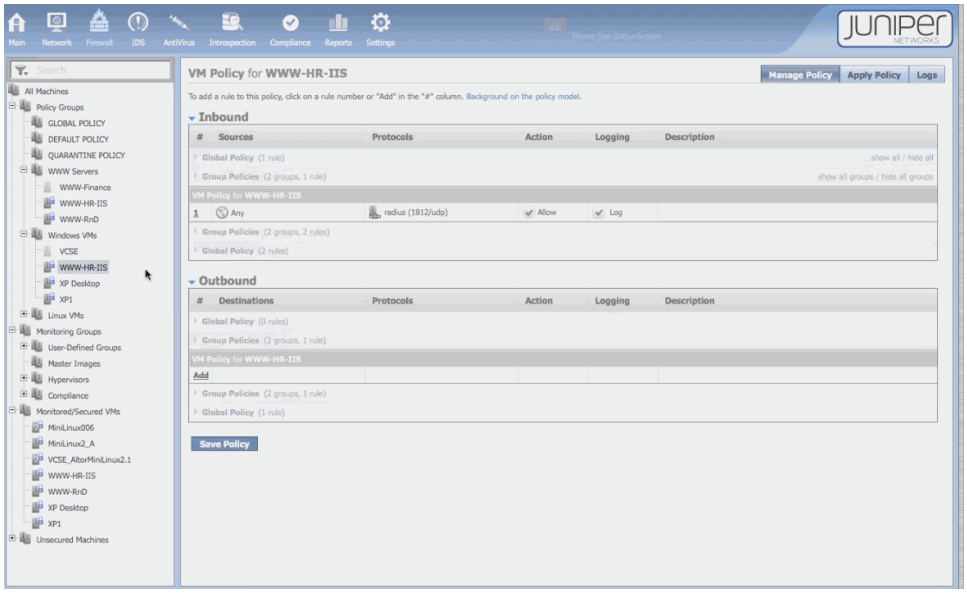
   TIP: **Because WWW-HR-IIS belongs to two groups, you can select it under either of its groups to display its VM Policy page.**

   The VM Policy for WWW-HR-IIS page is composed of the following nested parts that were previously built:

   - the high-level and lower-level Global Policy rules forming the outer layer of the nest.
   - a high-level Group Policy section below the high-level Global Policy. It states that the VM Policy contains two Policy Groups with a rule defined in only one of them.
   - a middle section called VM Policy for WWW-HR-IIS. You can add VM Policies specifically for the VM to this section.
   - the low-level Group Policy section that indicates that the VM belongs to two Policy Groups and that it inherits their Group Policies that include two rules.
   - the low-level Global Policy.

   Figure 21 on page 36 shows the policy.

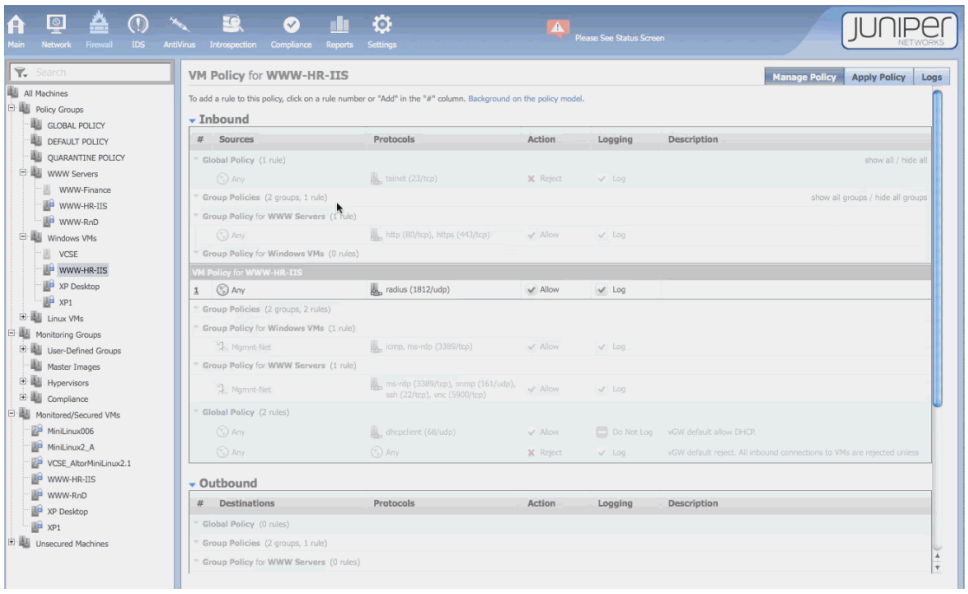
Figure 21: VM Policy for an Individual VM



2. To see the entire rule base for the VM, expanding the policies that it inherited to show their rules, click **show all** in the upper-right corner of the page.

   See Figure 22 on page 36.

Figure 22: Complete VM Policy for an Individual VM

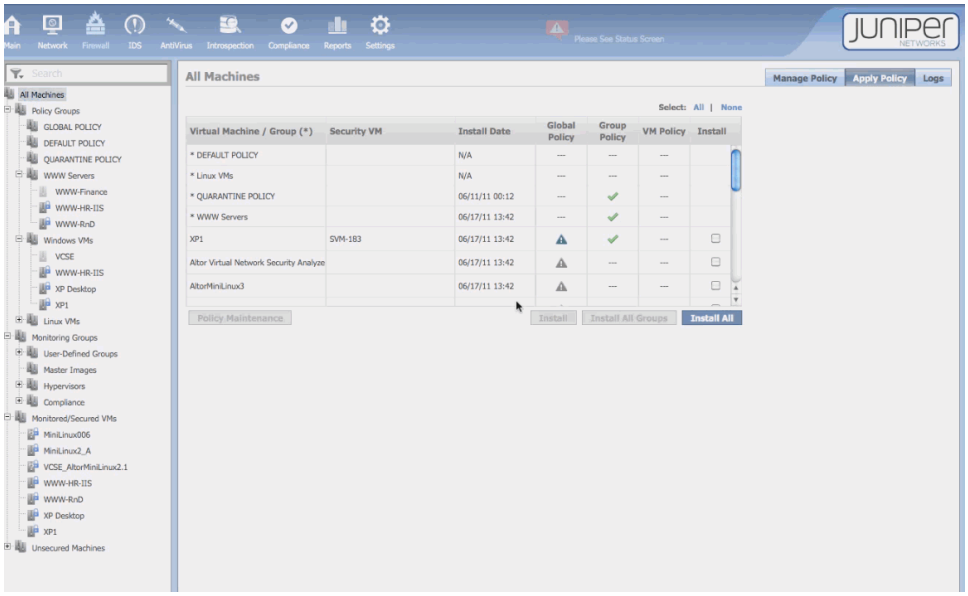


Copyright © 2015, Juniper Networks, Inc.

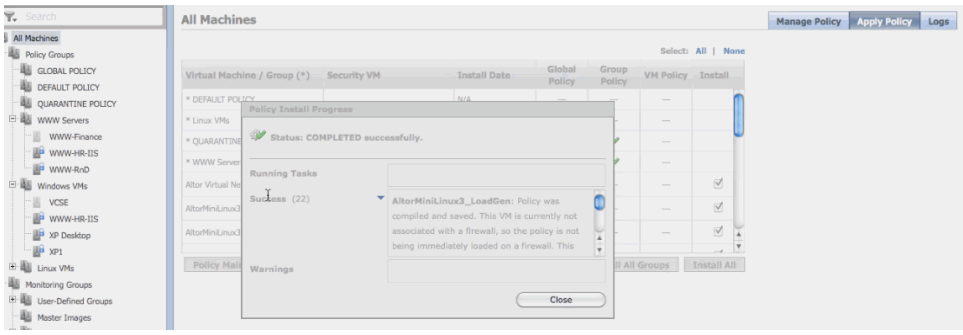
Apply the VM Policy.

When you define a firewall policy for a VM, it is not automatically applied. You must use the Firewall module Manage Policy tab to install it. This procedure installs a firewall policy for a single VM: AltorMiniLinux3.

1. Select the Firewall module. Select **All Machines** in the VM Tree. The following page is displayed.



2. Select the VM and click **Install**. In this example, All Machines is selected . After the firewall policy is installed on the VMs, the message shown in the following figure is displayed.



Related Documentation

- *Understanding vGW Series*
- Using the vGW Series Network and Firewall Modules Cooperatively on page 8
- Understanding vGW Series Predefined Firewall Policy for Its Components on page 38

Copyright © 2015, Juniper Networks, Inc.

Understanding vGW Series Predefined Firewall Policy for Its Components

vGW Series Firewall module allows you to secure virtual machines (VMs) within your virtualized infrastructure with individual policy rules, group policy rules, and global policy rules.

Not to be confused with securing VMs in your virtualized data centers, vGW Series secures and protects its own two main components—the vGW Security Design VM and the vGW Security VM—with predefined rule sets. You cannot change these predefined policy rules nor should you ever need to.

vGW Series stateful firewall comprises the following predefined rule sets for its two components.

For the vGW Security Design VM, the policy rules

- allow the following connections:
  - all outgoing connections
  - all incoming TCP/8443
  - all incoming TCP/443
  - all incoming TCP/8003
  - DHCP
  - NDP on IPv6
- Otherwise all connection attempts are dropped.

For the vGW Security VM, the policy rules

- allow the following connections:
  - all outgoing connections
  - all incoming TCP/8443
  - DHCP
  - NDP on IPv6
- Otherwise all connection attempts are dropped.

Related Documentation

- Understanding the vGW Series Firewall Module on page 11
- *Understanding the vGW Security Design VM*
- *Understanding the vGW Security VM*
- *Understanding vGW Series*

Copyright © 2015, Juniper Networks, Inc.

PART 2

IDS and AntiVirus

- IDS Module on page 41
- AntiVirus Module Basics on page 51
- vGW Endpoint for AntiVirus on page 69
- AntiVirus Scanning Config on page 75

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 3

IDS Module

- Understanding the vGW Series IDS Module on page 41
- Configuring IDS Settings and Viewing Activity on page 48

Understanding the vGW Series IDS Module

vGW Series includes a fully integrated IDS engine that you can use to monitor all virtual network traffic. It takes into account IPv4 and IPv6 traffic. You can also selectively monitor traffic for a subset of VMs or protocols used. vGW Series matches the selected traffic to the signature database and flags any suspicious activity with High, Medium, or Low priority alerts.

This topic covers the IDS module Alerts pages.

Use the Settings module > Security Settings > IDS Settings page to configure IDS for your environment. See *Understanding and Configuring IDS Settings*.

The IDS engine shows attacks generated by VMs or by external systems. The IDS engine can identify an attack when one party involved in the attack is a VM.

This topic includes the following sections:

- Managing and Sorting Displayed Alerts Information on page 41
- Top Alerts Page on page 42
- Alert Sources Page on page 47
- Alert Targets Page on page 47
- All Alerts Page on page 47

Managing and Sorting Displayed Alerts Information

By default, basic alerts information is displayed for all Alerts tabs. In basic mode, you can change the time interval to control the period for which alerts information is displayed. Also, you can click the displayed information column heads to sort alerts based on alert type, signature ID, total number of alerts of that type, or priority.

For all Alerts tabs, advanced mode gives you the following additional capabilities:

- You can enable Auto-refresh to direct vGW Series to refresh, or update, the alerts information displayed every 60 seconds.

Copyright © 2015, Juniper Networks, Inc.

- You can direct vGW Series to sort displayed alerts information based on alert level. You might want to quickly view only high alerts to assess the greatest danger. In that case, you can select High and remove the check mark from the check boxes for Medium and Low alerts.

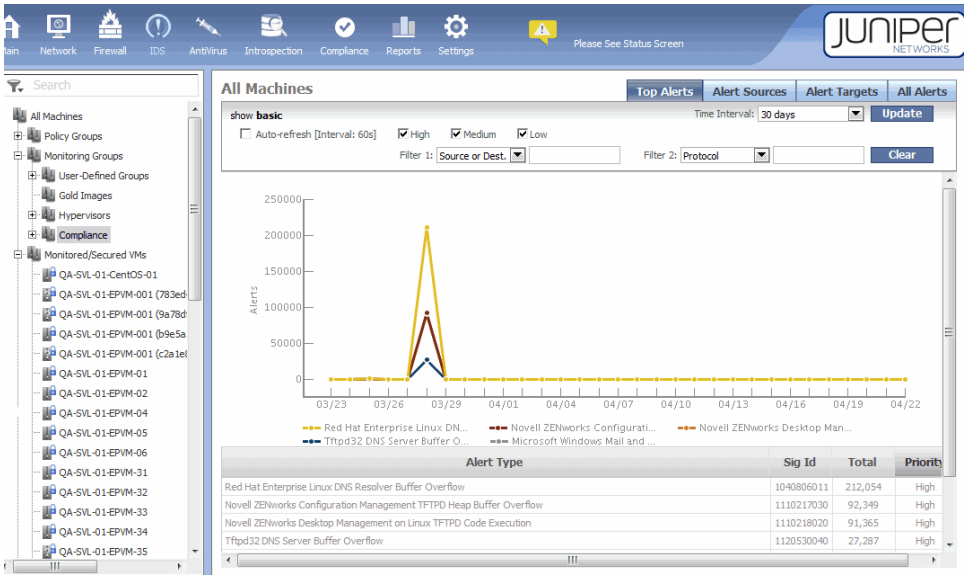
  You can show all alerts—High, Medium, and Low alerts—as basic mode does, or you can show only High, Medium, or Low alerts, or any combination of them.

- You can use the advanced filter capability to display alerts information based on two filter settings. Your first filter can direct vGW Series to sort alerts based on Source or Destination, alerts for both of them, or by Signature ID, Protocol, or Record ID. Your second filter could refine even further the information that is displayed, specifying one of these categories in conjunction with the first filter value. For example, you might want to sort alerts by signature ID and within that result sort by Source to look at a specific kind of event and the sources that generated the alert.

Top Alerts Page

The Top Alerts tab presents a graph that shows the top alerts for attacks that have occurred over a specified period of time, for example 24 hours. If you specify a different time interval, alerts that have occurred within that period of time are displayed. The graph allows you to view at a glance for each alert type the degree of frequency. It includes a table that identifies the type of alert and its signature ID. See Figure 23 on page 42

Figure 23: IDS Top Alerts

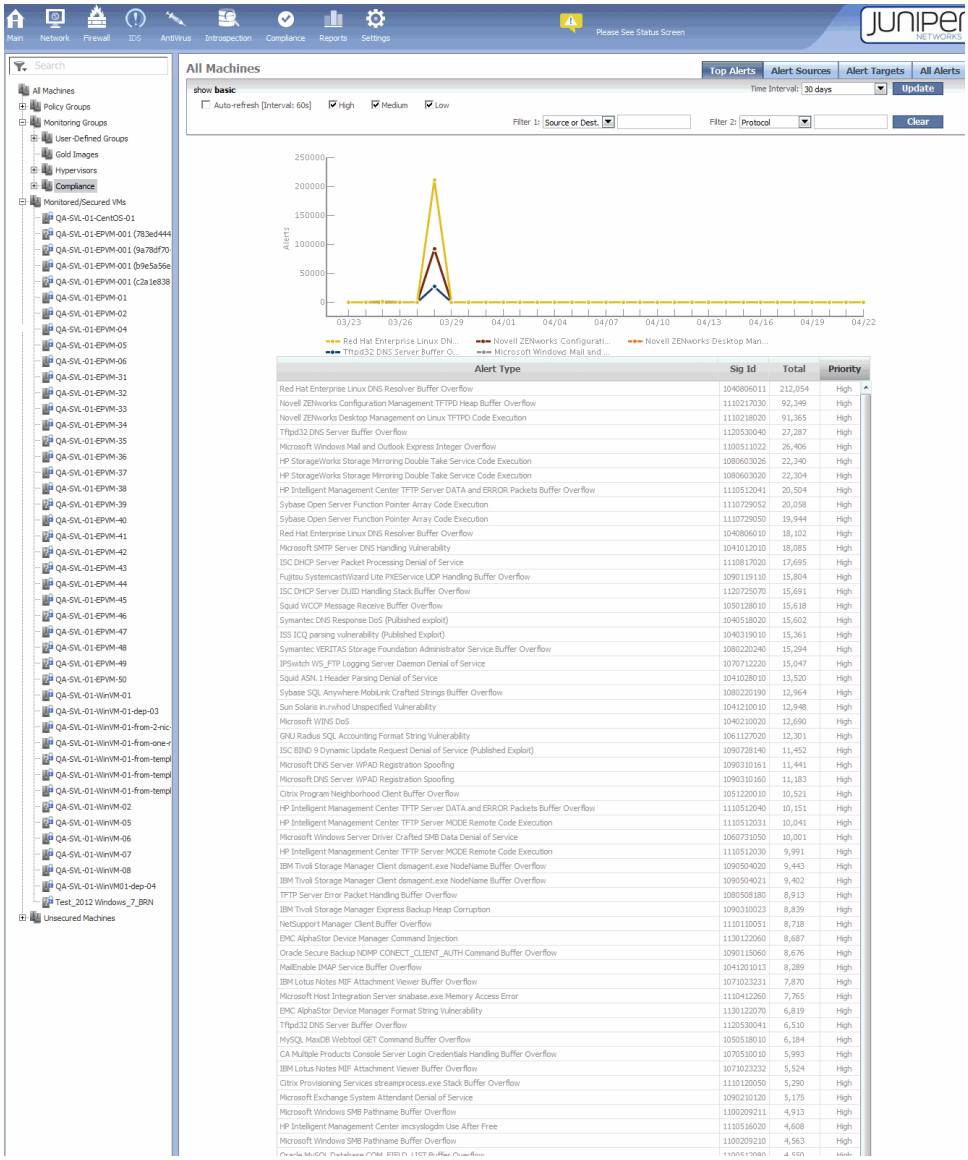


The alerts are organized as High, Medium, and Low with the total number sorting from most frequent to least frequent in the Total column.

To display advanced mode that gives you more options, click **show advanced**. Figure 24 on page 43shows the features that you can use in advanced mode with the time interval changed to reflect information for 30 days.

Copyright © 2015, Juniper Networks, Inc.

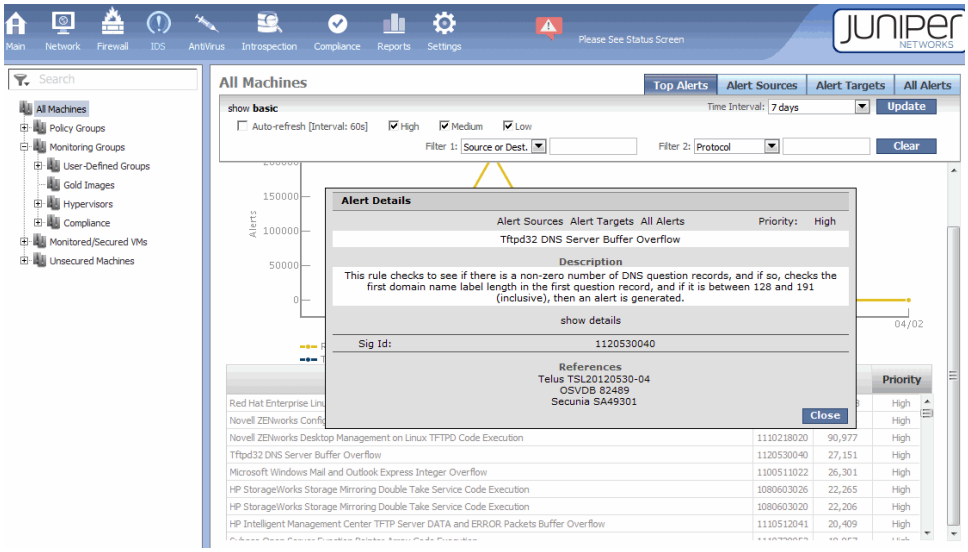
Figure 24: IDS Top Alerts Advanced Options



TIP: To change the priority level of an alert or not display information about it, use the Settings module > IDS Signatures page > Security Settings section.

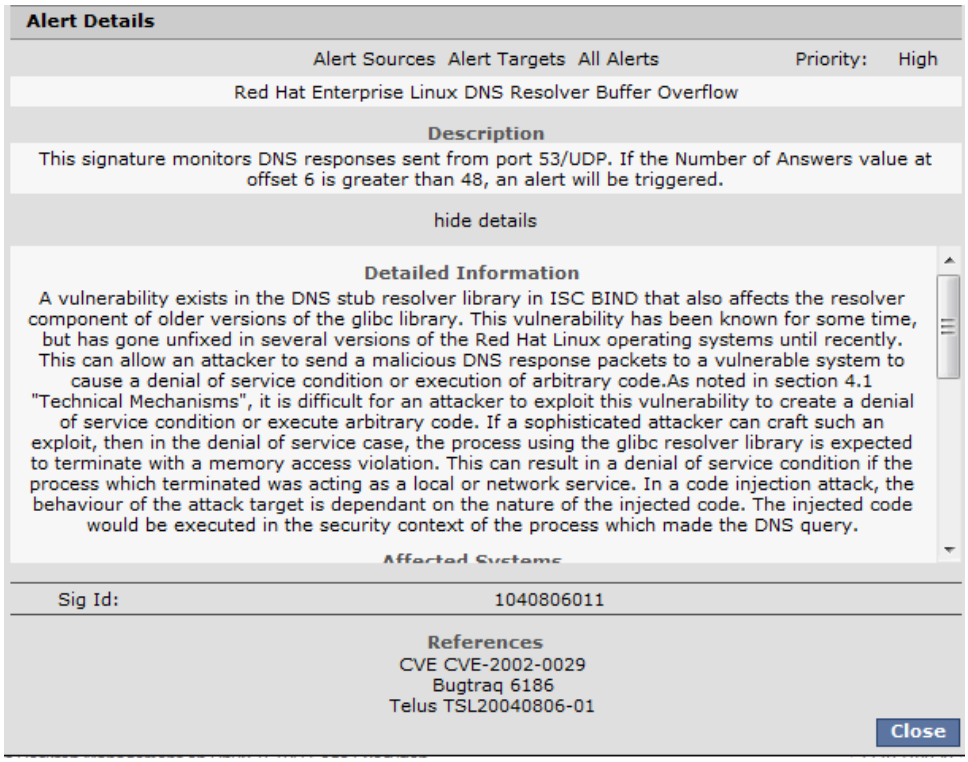
To show information about a specific attack that caused the alert, click its row in the **Alert Type** column. In response, you see a description of the alert and its signature ID. See Figure 25 on page 44.

Figure 25: IDS Alert Description



To show additional details for that alert, beneath the alert description click **show details**. Figure 26 on page 44 shows the result.

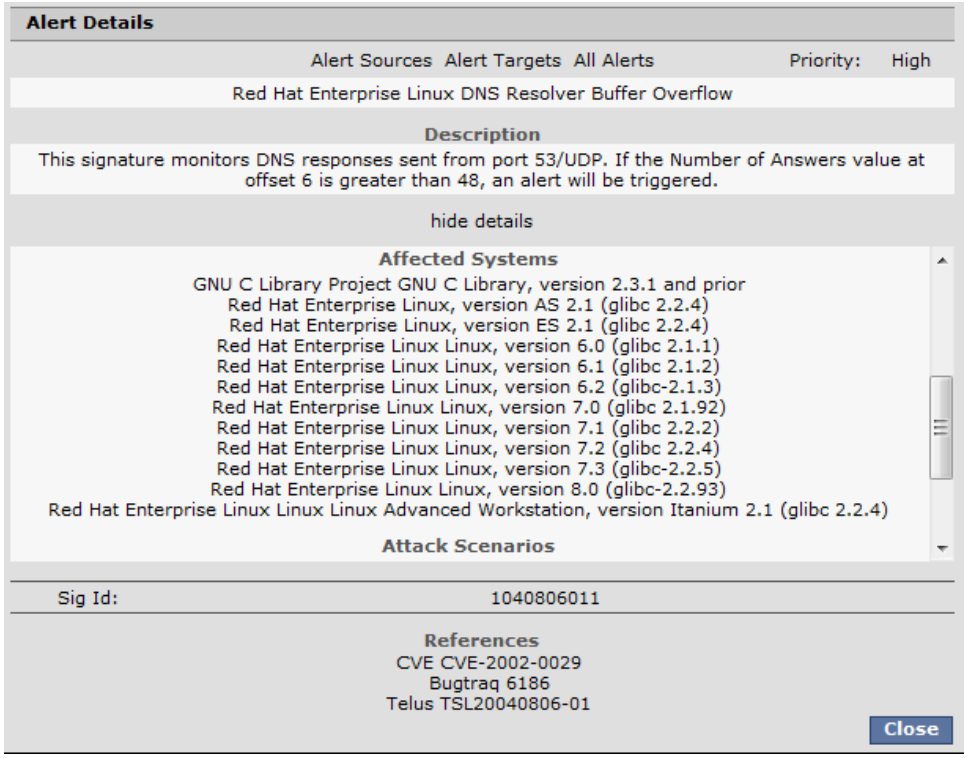
Figure 26: IDS Alert Details



Scroll down on the Alert Details box to see the affected systems and the attack scenarios. See Figure 27 on page 45.

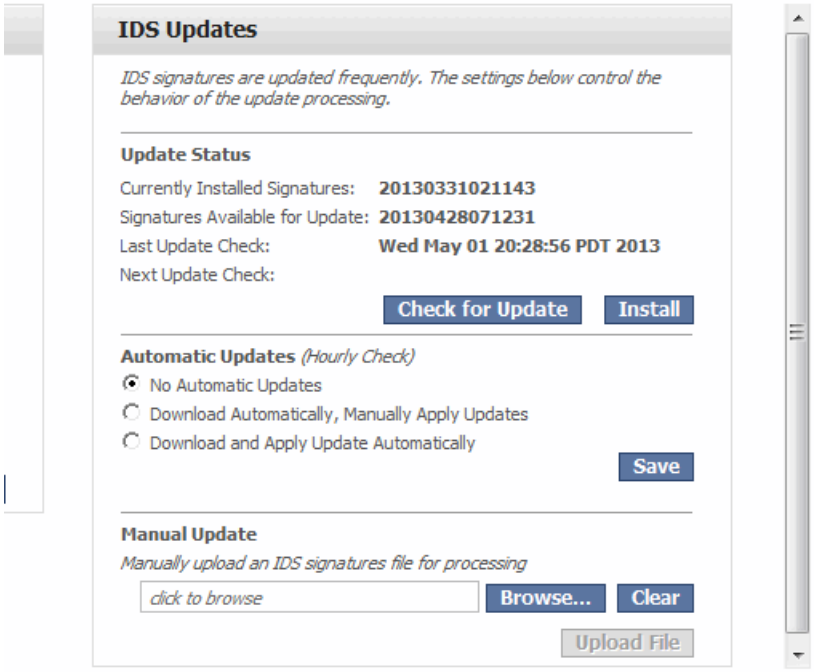
Copyright © 2015, Juniper Networks, Inc.

Figure 27: IDS Alert Details Showing Affected Systems



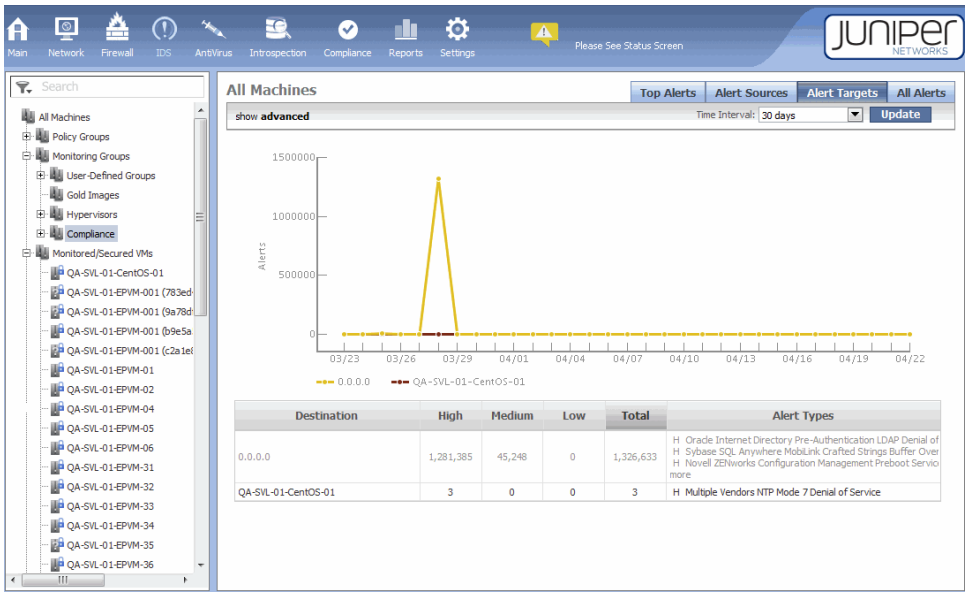
If you want to know who generated the traffic that caused an alert, click the **Alert Sources** tab. See Figure 28 on page 46.

Figure 28: IDS Alert Sources



If you want to know the traffic destination, click the **Alert Targets** tab. See Figure 29 on page 46.

Figure 29: IDS Alert Targets



Copyright © 2015, Juniper Networks, Inc.

Alert Sources Page

The Alert Sources window shows which systems have generated traffic matching the IDS signatures. These systems can be guest VMs or external systems communicating on the virtual network. The columns show High, Medium, and Low alert counts and a total count.

The system with the highest total count is displayed at the top of the list. You can sort the display by clicking the **High**, **Medium**, or **Low** columns. See Figure 28 on page 46.

Alert Targets Page

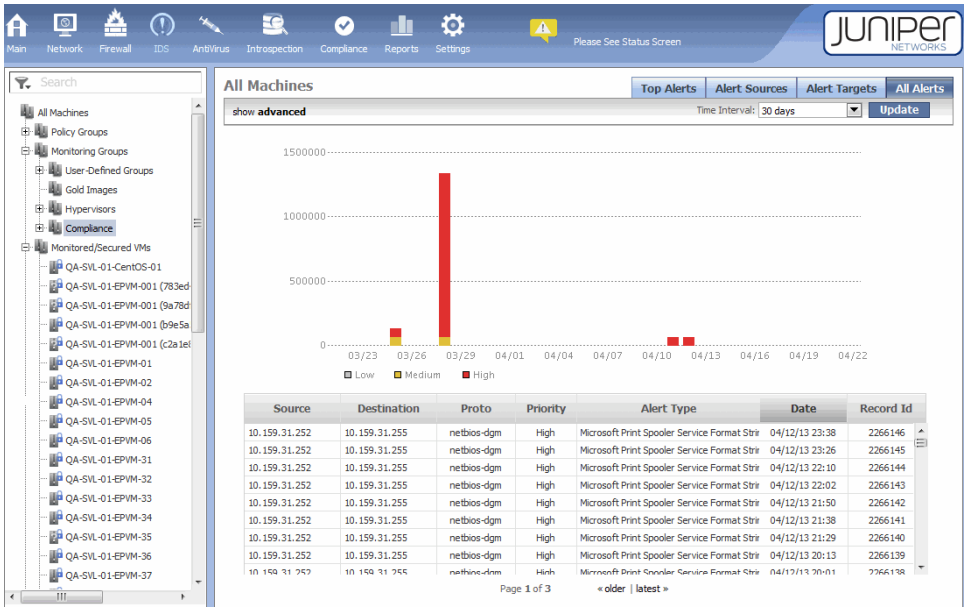
The Alert Targets window shows the same information as the Alert Sources page but also it shows a list of the systems that are under the greatest number of attacks. See Figure 29 on page 46.

All Alerts Page

The All Alerts tab shows a complete list of alerts for attacks captured by the system for the configured **time interval** (by default, 24 hours). In this example, the time interval has been set to 30 days.

To show details for a specific alert, click the alert type. By default, the most recent events are displayed at the top of the page, and older events are shown at the bottom. See Figure 30 on page 47.

Figure 30: IDS All Alerts



The Source and Destination columns in the All Alerts page table show machine names, not IP addresses. When you roll the mouse and hover over a machine name, vGW Series displays its IP address. To make it clear which IP address is involved, vGW Series displays only the IP address that the alert pertains to, not all IP addresses for that machine.

Copyright © 2015, Juniper Networks, Inc.

Machines for which IPv6 is enabled typically have two addresses bound to each Virtual Network Interface Card (vNIC)—a link local address and a routable address. Typically the link-local address is not used by applications. A machine can have multiple vNICs, each of which might have two IP addresses. Effectively a machine might have many IP addresses bound to it.

Related Documentation

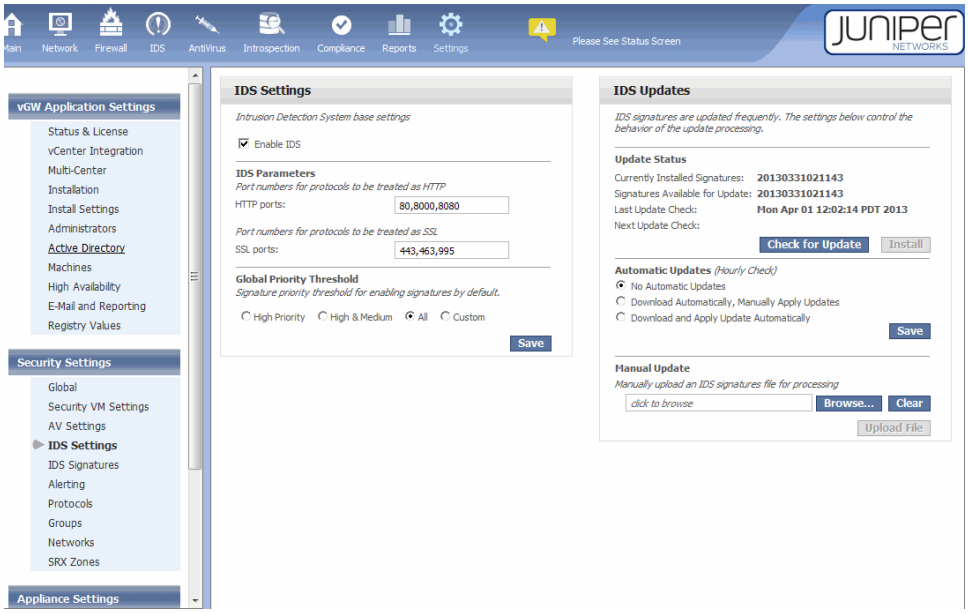
- *Understanding and Configuring IDS Signatures Settings*
- Configuring IDS Settings and Viewing Activity on page 48

Configuring IDS Settings and Viewing Activity

This topic covers how to configure IDS and view the results produced by the IDS engine.

1. Enable IDS and specify its settings using the Settings module Security Settings > IDS Settings > IDS Settings pane. See Figure 31 on page 48.

Figure 31: IDS Settings Page



2. Enable the signatures relative to your environment.

   From the Settings module, select Security Settings > IDS Signatures for a list of signatures.

   For details, see *Understanding and Configuring IDS Signatures Settings*

3. Create and apply a policy rule that mirrors traffic to the IDS engine. vGW Series gives you the ability to specify at a granular level which traffic to scan. For example, you might want to scan traffic to or from a specific VM, or traffic that uses a specific protocol.

Copyright © 2015, Juniper Networks, Inc.

NOTE: **Traffic that the firewall blocks is not inspected by the IDS engine because the connection is never established.**

A policy rule might be defined to inspect a connection for IDS but that does not imply that it accepts it. If the policy rule accepts, drops, or rejects a connection—all of which are considered terminal actions—policy scanning terminates. In this case, IDS rules that follow the rule that caused policy scanning to terminate are not processed. For IDS to take effect, the IDS rule for a connection must precede the rule that accepts the connection.

Related Documentation

- Understanding the vGW Series IDS Module on page 41
- *About the vGW Series IDS Reports*
- *Understanding and Configuring IDS Signatures Settings*

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 4

AntiVirus Module Basics

- Understanding vGW Series AntiVirus on page 51
- vGW AntiVirus Configuration Overview on page 58
- Understanding Quarantined VMs and How to Manage Them on page 65

Understanding vGW Series AntiVirus

This topic explains the vGW AntiVirus feature. vGW AntiVirus provides improved security and flexibility that agents alone cannot provide. It does this through:

- use of its kernel module installed in the ESX/ESXi host hypervisor.
- its management integration.
- its On-Access scans on VMs with only a light installation on the machine using its vGW Endpoint. An on-access scan is performed whenever a file is read from or written to disk.
- its On-Demand scans on VMs entirely without any installation on the VM and including no requirement to reconfigure the VM after the scan. vGW Series takes snapshot of the VM disk, and it performs the scan offline and deletes the snapshot that it takes and scans.

This topic begins by giving background information on antivirus technology. Then it explains vGW AntiVirus.

NOTE: **vGW Series AntiVirus feature requires a license.**

For an overview of the complete vGW AntiVirus configuration process, including information on mandatory preliminary configurations, read "vGW AntiVirus Configuration Overview" on page 58. For each step, the topic provides links to topics that give detailed procedures.

This topic includes the following sections:

- About Antivirus Software on page 52
- Signature-Based Detection on page 52
- The vGW AntiVirus Feature on page 52

About Antivirus Software

Antivirus software prevents and detects malware, such as viruses, worms, and spyware. A variety of strategies are usually involved in implementing antivirus software, including use of signature-based detection and rootkit detection, both of which the vGW AntiVirus supports.

Virtualized environments experience the same persistent threats and proliferation of malware that physical networks do. Not uncommonly, administrators of physical networks who have virtualized their environments install the same antivirus software that they use on their hardware desktops on their virtual machines. When it is installed on virtual systems, antivirus software designed for physical environments is severely limited, and it creates many problems. It does not recognize the virtual infrastructure; it consumes excessive memory usage, often exceeding 100 MB of RAM for a single guest VM; and it heavily degrades system performance through exhaustive CPU usage, often resulting in what is referred to as *brownout*.

Antivirus software is often the first line of defense against malware, but it should not provide this protection in the virtual environment at the cost of system performance.

Signature-Based Detection

A signature is a unique string of bits, or a byte pattern, that is characteristic and part of a certain virus or group of viruses. During a virus scan, the vGW AntiVirus feature compares the content of resources and files to be scanned against its virus signature database.

When vGW Series detects a signature pattern, it takes the remediation action that you specify when you configure the vGW AntiVirus scan. You use the vGW AntiVirus module's Scanner Config tab, which allows you to specify more than one action, for this configuration.

For example, when you select **Alert when a virus is detected** as an action, the Virus Alerts tab shows details on the event when vGW AntiVirus detects a virus. You can view the Virus Alerts tab content to gain an understanding of the types of threats that have been found, such as worm.exe, and where the threat was identified, such as the workstation name and other related information.

The vGW AntiVirus feature is robust in that it uses two methods to detect viruses and malware. It uses a signature database to detect specific viruses. It complements this approach with heuristics methods for detecting suspicious code parts.

The vGW AntiVirus Feature

Traditionally and extending into the present, antivirus software for the physical environment was developed to protect either the host—your desktop, servers, and other local devices—or the network for which malware and attack attempts could be caught before they reached the host.

Software for the desktop, and other hosts, is thought of as agent, or endpoint, software. Endpoint software involved installing a scanning engine and an attack signature database on every machine, which results in slower system startup and performance on the device.

Copyright © 2015, Juniper Networks, Inc.

When device scans run, memory is consumed and performance is affected. This model was carried into the virtualized environment as security products began to become available for it; the virtualized network and the virtualized host were protected separately by separate products.

The vGW AntiVirus feature constrains performance impact on the VM in both cases by centralizing its scanning engine and signature database on the vGW Security VM firewall instantiated on each ESX/ESXi host for which you configure vGW AntiVirus, and not on each VM. For On-Access scanning, whenever a VM's disk is written to or read from, the "lightweight" vGW Endpoint that you install on it passes several portions of the file necessary to determine if it contains a virus to the vGW Security VM across the virtualized network for examination.

The vGW AntiVirus feature remains effective when VMware VMotion is used. When a VM that is protected by vGW AntiVirus is migrated to another ESX/ESXi host through VMotion, the VM remains protected. The vGW Security VM on the host to which it is moved takes up the vGW AntiVirus protection work, based on the original configuration.

The vGW AntiVirus feature protects VMs by detecting malware, quarantining affected VMs and for On-Access scans also quarantining affected files. It allows you to define a remediation plan.

When you enable the vGW AntiVirus feature, the vGW Security Design VM activates its scanning engine on the vGW Security VM. This approach centralizes the scanning engine to limit disk, disk I/O, memory, and CPU consumption, and distribute the load across the virtualized infrastructure. The vGW AntiVirus database and the updates to it are also deployed on the vGW Security VM.

vGW AntiVirus relies on three main components:

- vGW Security Design VM

  You use the vGW Security Design VM to enable vGW AntiVirus, configure scans, view reports and alerts, download new signature versions, and download the vGW Endpoint.

  If the vGW Security Design VM is configured for dual stack, first it attempts to use the IPv4 protocol to communicate with the vGW Security VM.

  NOTE: By default, a dual stack vGW Security Design VM communicates with a vGW Security VM using the IPv4 protocol. However, you can use the vGW CLI to change the default IP protocol used by setting the center.dual.stack.default.communication.ipv4 parameter to false.

  center.dual.stack.default.communication.ipv4=false

  By default, this parameter is set to **true**.

  This parameter is relevant only if the vGW Security Design VM is configured for dual stack and one or more vGW Security VMs is also configured for dual stack. In all other cases, the protocol used is the one that is common to both the vGW Security Design VM and the vGW Security VM, and this parameter is irrelevant.

- vGW Security VM

  The vGW Security VM performs On-Demand scans.

  It is possible to perform an On-Demand scan on a VM whose ESX/ESXi host does not have a vGW Security VM installed. In this case, the scan is performed by the vGW Security Design VM, a vGW Security VM on a different host (TCP 902 is required), or both.

  vGW AntiVirus remains in effect when a VM is VMotioned to another host for analysis. In that case, the vGW Security VM on that host performs the vGW AntiVirus functions.

- vGW Endpoint

  The vGW Endpoint is used for On-Access scans. It protects a VM against infected files whenever a file is read from or written to disk. The vGW Endpoint sends the file to the vGW Security VM to be analyzed.

  When an infected file is identified and the quarantine action is specified in the On-Access scanner configuration, the file is isolated in the vGW Endpoint on the VM. It remains there until you *un-quarantine* it, delete it, or fetch it. When you release it from quarantine, it is made available to the VM again.

NOTE: **On-Demand scans do not require installation of the vGW Endpoint. The vGW Endpoint is used for On-Access scans only.**

vGW Series supports both AntiVirus On-Demand and On-Access features in IPv4 or IPv6 environments, or environments that are a mix of the two.

Although the vGW AntiVirus works in an IPv6 environment, communication between the vGW Endpoint and the vGW kernel module installed in the ESX/ESXi host hypervisor occurs over the IPv4 infrastructure. Note that the vGW Endpoint OS should be configured with the IPv4 stack enabled.

The vGW AntiVirus Dashboard

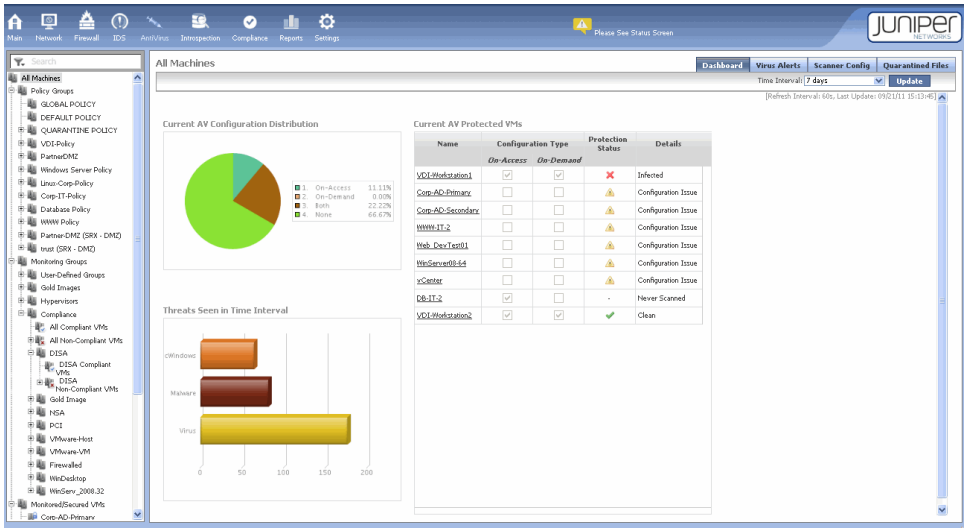
The vGW AntiVirus dashboard gives you an overall view of the current state of all protected VMs in your environment.

- You can view information for all VMs in your environment or for specific VMs. You use the VM tree to select the VMs.
- You can change the time interval to view threats that occurred within a broad or narrow span of time.
- You can view information on vGW AntiVirus events for VMs, such as details on viruses that were detected and signature updates.

Figure 32 on page 55 shows the vGW AntiVirus Dashboard.

Copyright © 2015, Juniper Networks, Inc.

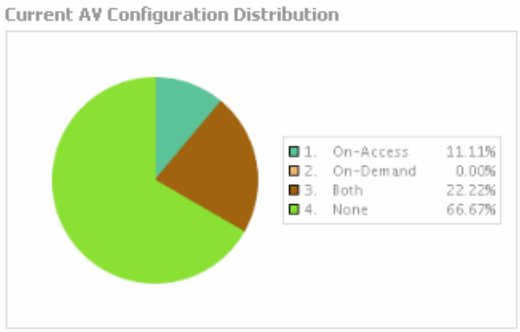
Figure 32: vGW AntiVirus Dashboard



The vGW AntiVirus Dashboard includes these panes:

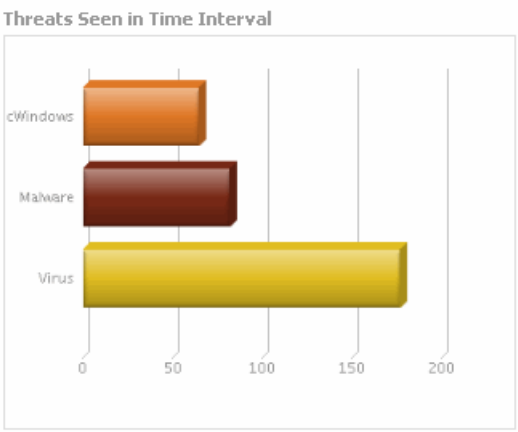
- Current vGW AntiVirus Configuration Distribution

  This pie chart shows you proportionally the number of VMs that are protected by the On-Access scanner, by the On-Demand scanner, or both of them, and those that are not protected by vGW AntiVirus.



- Threats Seen in Time Interval

This bar graph display the kinds and percentage of threats that were identified in the selected time interval.

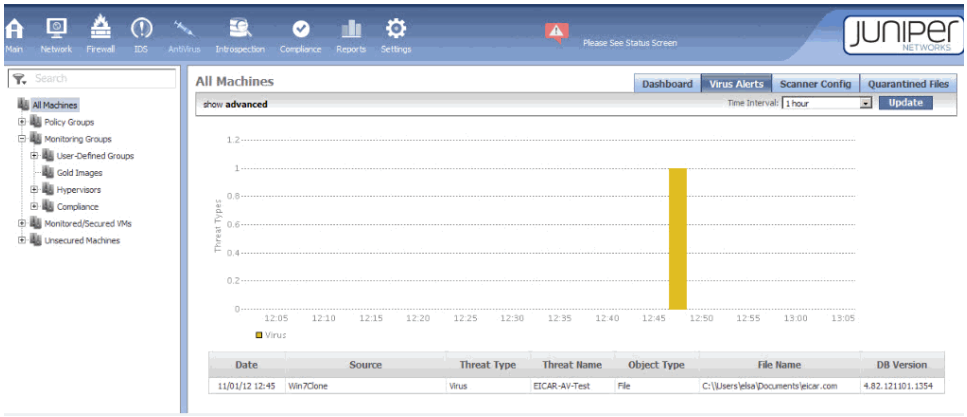


- Current vGW AntiVirus Protected VMs

  This table identifies VMs that are protected by vGW AntiVirus, the type of scanner configurations that protect them, and the protection status and details for the VM. If the protection status indicates problems, you can click the VM's row to display a page dedicated to it giving detailed information. The page shows scan statistics for the VM (how many files were scanned, how many files were quarantined, and so on), the scanner configuration for the VM, the threat type bar graph as applied to the VM, and a table identifying attempted virus infections, when they occurred, and how vGW AntiVirus handled them.

The Virus Alerts tab displays a graph that identifies threat types over a period of time. You use the Time Interval box to control the period. It gives details on the threat type, including the date of the event, the source, and the filename.

Figure 33: Virus Alerts

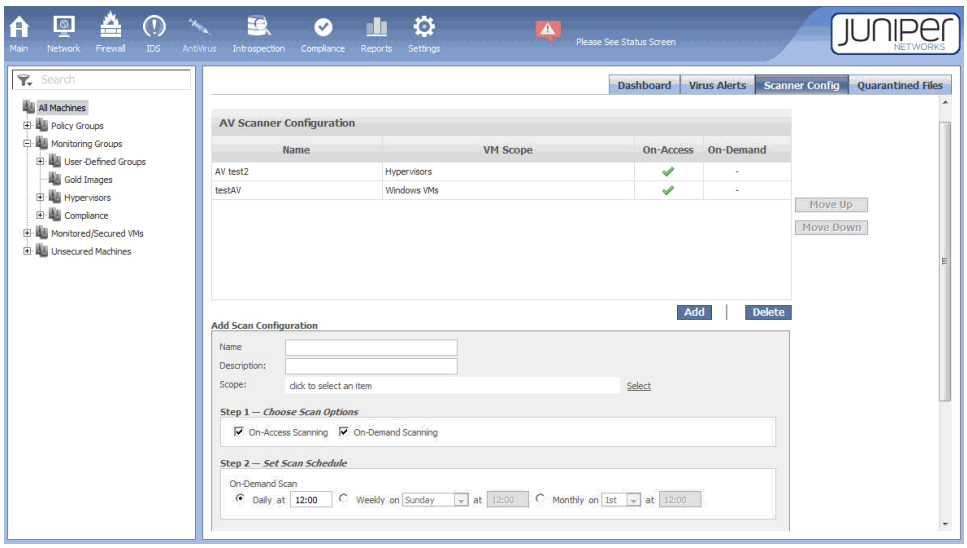


The Scanner Config page allows you define On-Access and On-Demand scans. When you click **Add** to display the Add Scan Configuration pane, both types of scans are selected. You can configure them separately or together in one configuration. You can configure a typical scan or a custom scan. Figure 34 on page 57 shows them configured together

Copyright © 2015, Juniper Networks, Inc.

by default with a typical scan used. For details on configuring them separately, see "Configuring vGW Series AntiVirus On-Access Scanning" on page 75 and "Configuring vGW Series AntiVirus On-Demand Scanning" on page 78.

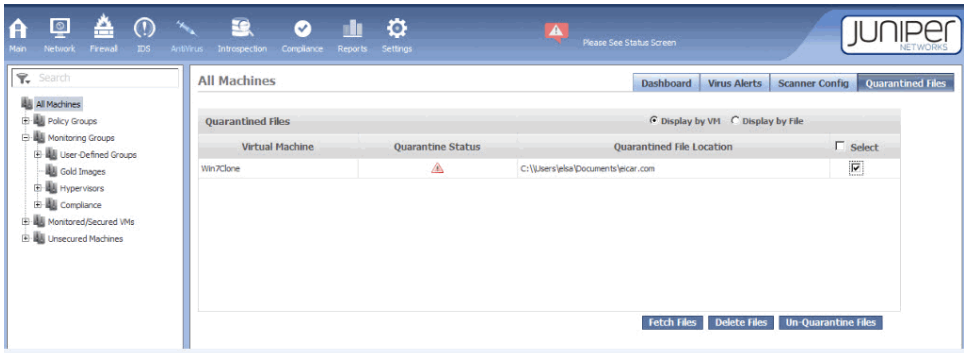
Figure 34: vGW AntiVirus Scanner Config Tab



The Quarantined Files tab displays a list of quarantined files. Only infected files identified through an On-Access scan can be quarantined. When a file is quarantined, it is isolated in the vGW Endpoint on the VM and information about it is displayed on this page. The VM containing the file is identified. The location of the file is shown and its status is noted. See Figure 35 on page 57.

NOTE: There must be no items for a VM in quarantine for that VM to appear as non-infected, or in a "clean" state, on the dashboard. However, if a VM is not quarantined and none of its items are quarantined does not mean that the VM is clean. If a VM has items in quarantine is not considered clean.

Figure 35: Quarantined Files



You can select one or more files and perform any of the following actions:

- You can fetch the file. In this case, the file is hashed and transferred off the VM for further analysis.
- You can un-quarantine the file. In this case, the isolated file is made available again to the VM.

  In some cases, files are quarantined because of false positive results. That is, the file is suspected of being malware or infected, but that is not the case. Updating the signature database and running the scan again often resolves the problem.
- You can delete the file from the VM if you have confirmed that the file is infected or that it is malware.

When a VM is infected by a virus and the scanning configuration specifies **Quarantine the VM**, the VM is put in the quarantine policy group. To remove the VM from the quarantine policy group, use the Main module Quarantine tab. Select the VM, and click **Un-quarantine**.

For details on how the parts of the quarantine process work together for a quarantined VM, see "Understanding Quarantined VMs and How to Manage Them" on page 65.

Related Documentation

- Understanding and Installing the vGW Endpoint on page 69
- *Understanding vGW Series*
- *Understanding and Configuring the vGW Series AntiVirus Settings*
- Configuring vGW Series AntiVirus On-Access Scanning on page 75
- Configuring vGW Series AntiVirus On-Demand Scanning on page 78

vGW AntiVirus Configuration Overview

This topic gives an overview of the steps to follow to configure vGW AntiVirus protection for your virtualized environment.

NOTE: **The vGW AntiVirus feature requires a license.**

For vGW Series to scan a VM, the VM must be included in one of the VM groups that you include in the scan scope, which you define when you configure a scan. You use the AntiVirus module Scanner Config page to configure scans. If a VM is not included in one of the groups in the scope, it will not be protected by vGW AntiVirus. You can define at a granular level the files on a VM to be scanned based on file type and file location. For example, you can configure a scan to scan all file types, only certain file types, files at all locations or only files at certain locations. You can combine these options, for example, to scan all file types but only at a certain location. You can also refine the scan by excluding types of files or files at certain locations from it.

vGW AntiVirus provides two means of protecting your environment against malware and viruses:

- The On-Access Scanner

 Copyright © 2015, Juniper Networks, Inc.

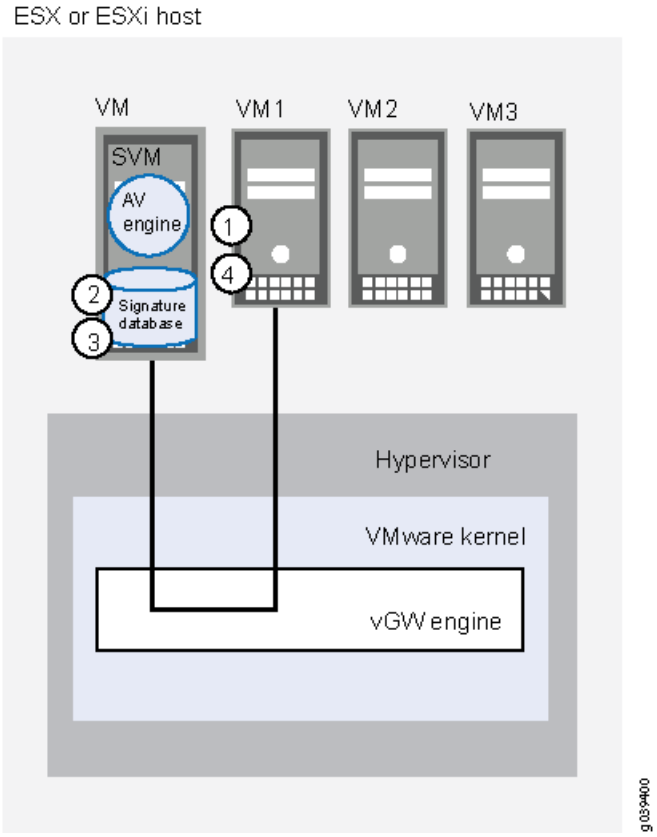
To protect VMs against malicious content and virus infections in real-time, the On-Access scanner runs whenever a VM's disk is written to or read from. It scans areas of the disk based on your configuration.

- When you configure a custom On-Access scan, you can specify file types and the location of files to scan. You can also exclude certain types of files and files at certain locations from the scan.
- You must specify the drive when you specify the location of files to scan for custom On-Access scans. For On-Access scans, when scanning files based on location, vGW Series takes into account the drive letter of the directory. For example, given the file location C:\Program, an On-Access scan scans files only in that directory. It does not scan files in the D:\Program directory, although the directory names are the same, because it acknowledges that the drive letters are different.
- For On-Access scans, vGW Series does not support the use of wildcards in file extensions or file locations.

Copyright © 2015, Juniper Networks, Inc.

Here is how the vGW AntiVirus On-Access scanner works, as illustrated in Figure 36 on page 60.

Figure 36: On-Access Scan



1. vGW Series installs a small agent called the vGW Endpoint on the VM when On-Access scanning is configured.

2. The vGW Endpoint captures file accesses and forwards them to the vGW Security VM on the host to scan.

   The file transfer is controlled internally, based on its match against the AntiVirus signatures. Only as much of the file as is necessary to determine if it is malicious is forwarded to the vGW Security VM. The vGW Security VM scans the file to make the determination. You cannot control this from the vGW Security Design VM.

3. An On-Access AntiVirus scan is performed.

   The vGW Security VM scans the file to make the determination.

   Because the scan is performed on the vGW Security VM, it is not necessary to re-configure a VM after an On-Access scan.

4. The scan results are cached in the vGW Endpoint for improved performance.

For details on how to configure On-Access scanner, see "Configuring vGW Series AntiVirus On-Access Scanning" on page 75.

Copyright © 2015, Juniper Networks, Inc.

- The On-Demand Scanner

  The On-Demand scanner performs full-disk offline scanning that scans VMs periodically, examining their virtual disk files for malicious content. You configure a schedule to specify when scanning should occur.

  On-Demand scans are performed without any impact to the VM. The scanning is done outside the VM on the ESX/ESXi host's vGW Security VM. Therefore it not necessary to re-configure a VM after an On-Demand scan.

  Here is how the vGW Series On-Demand scanner works:

  1. vGW Series takes a snapshot of the VM disk to be scanned.
  2. It attaches the snapshot to the vGW Security VM.
  3. Based on your Scanner Config for On-Demand scans, it performs either a typical scan or a custom scan. For a custom scan, it scans the archives, file types and file locations that you specify, excluding any file types or locations that you specify in your custom scan configuration.
  4. After it completes the scan, vGW Series detaches the snapshot from the vGW Security VM.
  5. Finally, it deletes the snapshot.

  Take into account the following characteristics when you configure a custom On-Demand scan:

  - vGW Series recognizes the global wildcards * and ?.

    For example, you could specify C:\Program Files\MS*. You could also use the wildcard on an extension, for example doc*.

  - For file locations, drive letters are ignored. For example, C:\Program Files matches:

    C:\Program Files and D:\Program

    vGW Series performs an On-Demand scan offline and does not take into account drive letters.

When you configure the vGW AntiVirus scanner, you can specify the action to take in response to results of the scan. Both On-Access and On-Demand scanning can result in a quarantined VM. However, files can be quarantined only as a result of an On-Access scan.

You can configure both On-Access Scanning and On-Demand Scanning in a single vGW AntiVirus scanner configuration.

You use the vGW AntiVirus module tabs in concert:

- to gain an overall, quick status on your environment as it stands in relation to vGW AntiVirus protection.
- to enact scanning.

- to identify files for which there are issues that need to be addressed and files that are quarantined.

  For details on how quarantined VMs are treated, see "Understanding Quarantined VMs and How to Manage Them" on page 65.

Figure 37 on page 62 shows the vGW AntiVirus dashboard that gives you a comprehensive view of vGW AntiVirus protection for your environment. It emphasizes a table that shows vGW AntiVirus details on individual VMs, including the kind of vGW AntiVirus protection it has and the current scan status on the VM. The dashboard also presents a pie chart that shows the vGW AntiVirus protection distribution across VMs. It includes a chart that shows the types and degrees of threats identified by vGW AntiVirus across a specific period of time, which you can adjust.

NOTE: There must be no items for a VM in quarantine for that VM to appear as non-infected, that is,in a "clean" state, on the dashboard. However, simply because a VM is not quarantined and none of its items are quarantined does not mean that the VM is clean. But you can be assured that it is never the case that a VM that has items in quarantine is clean.

Figure 37: vGW AntiVirus Dashboard

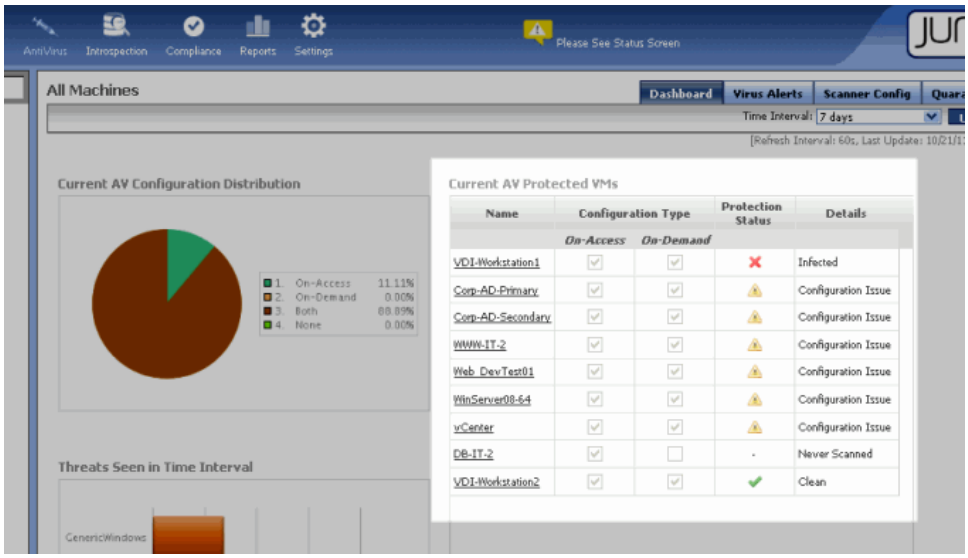
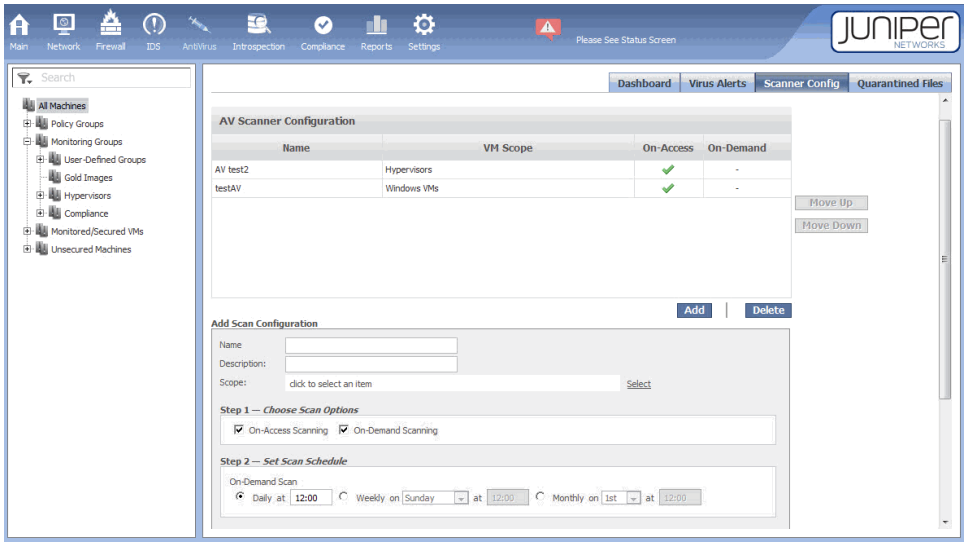


Figure 38 on page 63 shows the two scanning options that you can configure using the Scanner Config tab.

Copyright © 2015, Juniper Networks, Inc.

Figure 38: Scanner Config Tab



A vGW AntiVirus On-Access scan can result in quarantined files or VMs:

- Quarantined files are identified in the vGW AntiVirus module Quarantine tab.
- Quarantined VMs are identified in the vGW Main module Quarantine tab.

Complete these prerequisite tasks:

1. Secure the ESX/ESXi hosts. Deploy the vGW Security VM out to the ESX/ESXi hosts in your environment. From the Settings module, select **vGW Application Settings > Installation** for this purpose. See *Installing vGW Security VMs on ESX/ESXi Hosts*.

   If you do not deploy the vGW Security VM and you protect the VMs with the vGW firewall, On-Access scanning will not work. Configuring only the On-Access scanner for the VMs and enabling vGW AntiVirus is ineffective without this preliminary configuration.

2. Secure the VMs. Configure the vGW Firewall for VMs that you want to protect with On-Access scanning. From the Firewall module, select the **Manage Policy** tab to create firewall policies and the **Apply Policy** tab to apply them. See "Understanding the vGW Series Firewall Module" on page 11.

To configure vGW Series On-Access scanning for your environment, you must:

1. Create an On-Access scanner configuration for the VMs.

   See "Configuring vGW Series AntiVirus On-Access Scanning" on page 75.

   NOTE: **When you configure an On-Access scan, you do not configure a scanner schedule. On-Access scanning occurs in real time.**

2. Enable the vGW AntiVirus feature and download the vGW Endpoint.

See *Understanding and Configuring the vGW Series AntiVirus Settings*.

3. Install the vGW Endpoint on the VMs to be protected.

   See "Understanding and Installing the vGW Endpoint" on page 69. This topic explains how to install the vGW Endpoint on VMs, and it explains the pop-ups that the vGW Endpoint displays to inform you about various conditions, such as when a threat is detected.

NOTE: **You must install the vGW Endpoint on all VMs that you want to protect with On-Access scanning.**

On-Demand scanning differs from On-Access scanning in the following ways:

- It is not possible to quarantine files when On-Demand scanning is used.
- You can run an On-Demand scan on VMs whose ESX/ESXi is not protected by the vGW Security VM. In this case, the scan is performed by the vGW Security Design VM, a vGW Security VM on a different host, in which case TCP 902 is required, or both.
- You do not need to install the vGW Endpoint on the VMs.
- For On-Demand scanning, you can protect VMs to be scanned with the vGW Firewall, but it is not required.

Because you do not need to protect VMs with the vGW Firewall and you do not need to install the vGW Endpoint on the VM, On-Demand scans can be performed on virtual disk files from a protected location that is not compromised. This advantage increases the ability of the vGW Series to detect and locate rootkits. It can detect files with suspicious names such as mal.exe, simpletroj.exe, and other malware files.

To configure On-Demand scanning:

1. Create an On-Demand scanner configuration for the VMs.

   See "Configuring vGW Series AntiVirus On-Demand Scanning" on page 78.

2. Enable the vGW AntiVirus feature.

   See *Understanding and Configuring the vGW Series AntiVirus Settings*.

Related Documentation

- Configuring vGW Series AntiVirus On-Access Scanning on page 75
- *Understanding and Configuring the vGW Series AntiVirus Settings*
- Understanding and Installing the vGW Endpoint on page 69
- Understanding vGW Series AntiVirus on page 51
- *Understanding Quarantined VMs and Files Resulting from a vGW AntiVirus On-Access Scan*
- Configuring vGW Series AntiVirus On-Demand Scanning on page 78
- *Understanding the vGW Security VM*

Copyright © 2015, Juniper Networks, Inc.

- *Understanding vGW Series*

Understanding Quarantined VMs and How to Manage Them

This topic covers aspects of the vGW Series quarantine feature. When a VM is quarantined as a result of a vGW AntiVirus, Compliance, or Image Enforcer scan, the VM is added to the Quarantine Policy group in the VM tree.

When a VM is added to the Quarantine Policy group, the quarantine policy that you configured using the Firewall module is applied to it. After a VM is quarantined, at any time, you can use the Main module Quarantine tab to manage it in various ways.

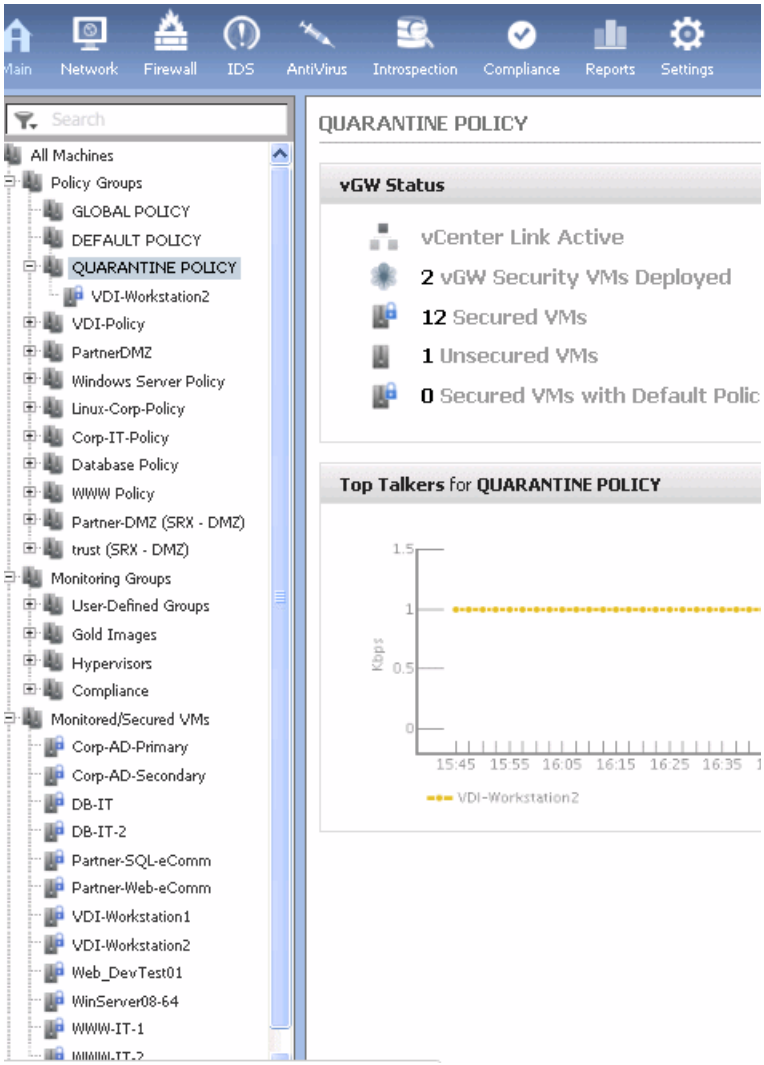
The Quarantine Policy group, the quarantine policy associated with it, and the Main module Quarantine tab cooperate to help you control and manage quarantined VMs. This topic includes the following sections:

- About vGW Series Quarantine on page 65
- Configuring a Quarantine Policy on page 66
- Viewing the Quarantined VMs, Releasing Them From Quarantine, and Resolving Problems on page 67

About vGW Series Quarantine

The Quarantine Policy group belongs to the Policy Groups branch. Figure 39 on page 66 shows that one quarantined VM has been added to the Quarantine Policy group.

Figure 39: Quarantine Policy in the VM Tree

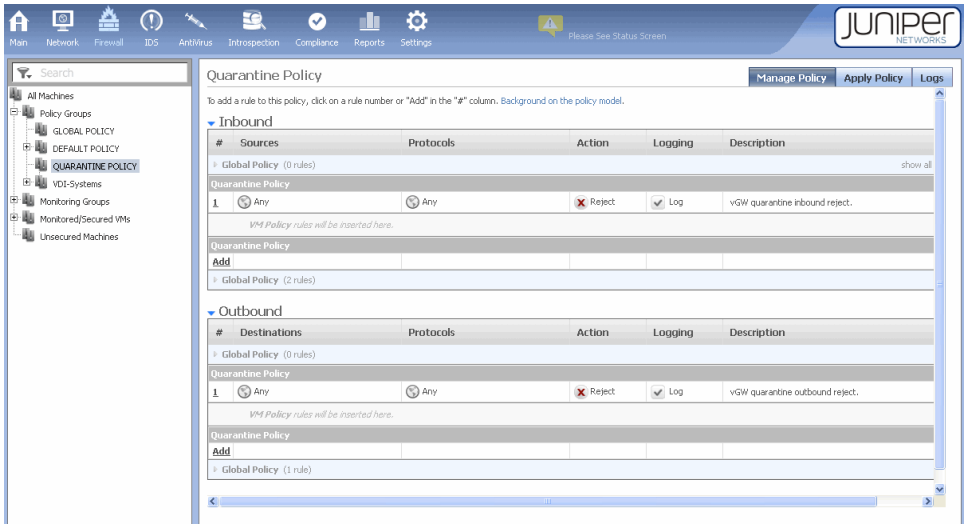


Configuring a Quarantine Policy

The Firewall module allows you to configure policy rules, including configuring a quarantine policy. You use the Quarantine Policy page for this purpose.

Copyright © 2015, Juniper Networks, Inc.

Figure 40: Configuring a vGW Series Quarantine Policy



To display the Quarantine Policy page:

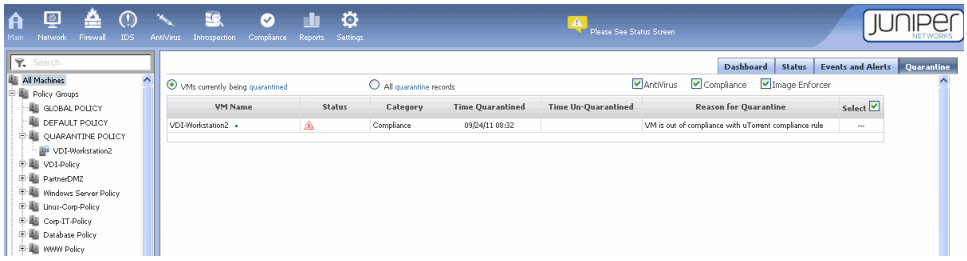
1. Select the Firewall module on the taskbar.
2. Select the Quarantine Policy group.
3. Configure the policy rules. For details on configuring policy rules, see "Understanding the vGW Series Firewall Module" on page 11.

Viewing the Quarantined VMs, Releasing Them From Quarantine, and Resolving Problems

The Main module Quarantine tab page displays a table that includes a row for each quarantined VM. You can display information for VMs quarantined as a result of vGW AntiVirus, Compliance, and Image Enforcer scans. You can display information for all quarantined VMs or VMs by scan category.

The table identifies the time the VM was quarantined and the reason for it. See Figure 41 on page 67.

Figure 41: Main Module Quarantine Tab



To view a quarantined VM in the quarantine table, resolve the problem, and remove it from quarantine:

1. Select the Main module in the taskbar.
2. Select the Quarantine tab.
3. To remove the VM from quarantine, select the VM and click **Un-Quarantine VM**.
4. Resolve the problem that caused the VM to be quarantined.

   Removing a VM from quarantine does not fix the underlying problem that caused the VM to be quarantined. A VM might be quarantined because of a compliance, image enforcer, or vGW AntiVirus violation.

   You can fetch the VM to resolve it offline or you can delete the VM.

Related Documentation

- *Understanding vGW Series*
- Understanding vGW Series AntiVirus on page 51
- Configuring vGW Series AntiVirus On-Access Scanning on page 75
- Configuring vGW Series AntiVirus On-Demand Scanning on page 78
- Understanding the vGW Series Enforcer Profiles Tab on page 95

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 5

vGW Endpoint for AntiVirus

- Understanding and Installing the vGW Endpoint on page 69

Understanding and Installing the vGW Endpoint

This topic explains the vGW Endpoint and how it is used. To understand vGW Endpoint download and installation procedures within the overall context of the vGW AntiVirus configuration, see "vGW AntiVirus Configuration Overview" on page 58.

WARNING: **IPv4 is required for the vGW Endpoint to work properly.**

- Installing the vGW Endpoint on page 69
- vGW AntiVirus Endpoint Auto-Update on page 69
- vGW Endpoint on the VM on page 70
- Quarantined Files on page 72
- vGW Endpoint Components and Displays on page 72
- vGW Endpoint Behavior on page 73

Installing the vGW Endpoint

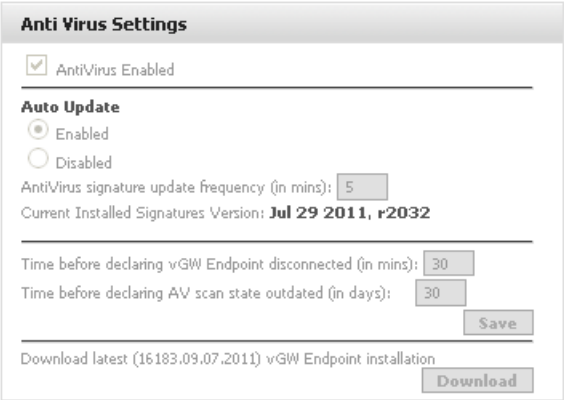
For vGW Series On-Access scans to be performed on a VM, a vGW Endpoint must be installed on each of the VMs belonging to the VM groups specified in the On-Access scanner configuration scope. The vGW Endpoint is a binary executable (.exe file) that you can install in various ways. For example, some administrators put binaries on a network share, in which case a login script maps the drive and executes the binary. Another way to install the binary is to post it on a Web server, and download and execute it as needed. In this case, you might want to use a software package such as Microsoft® Server and Cloud Platform System Center or Manage Engine Desktop Central. You can use whatever tools you prefer for this purpose.

vGW AntiVirus Endpoint Auto-Update

After you download the vGW Endpoint and distribute it to the protected VMs in your environment that you have included in the On-Access scanner configurations, you do not need to update it. When you update the vGW Security Design VM, it automatically

updates the vGW Endpoint on all VMs. That is, you install the vGW Endpoint once, and vGW Series auto-deploys an update. See Figure 42 on page 70.

Figure 42: vGW AntiVirus Settings

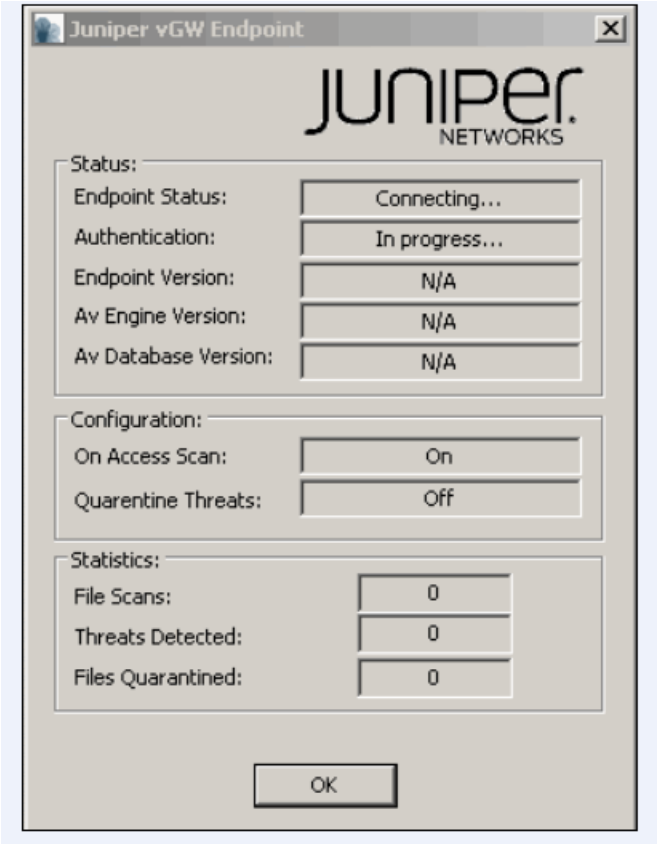


vGW Endpoint on the VM

When the vGW Endpoint is connecting to the vGW Series appliance, the following dialog box appears on the VM. See Figure 43 on page 71.

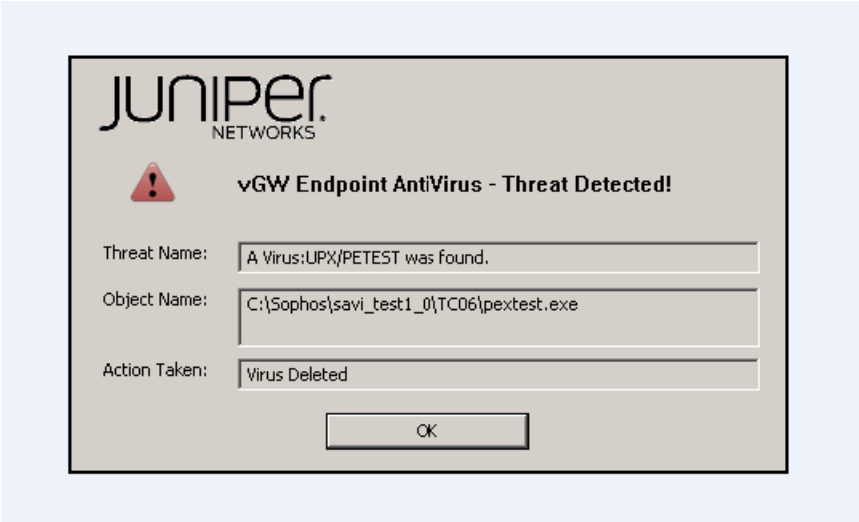
Copyright © 2015, Juniper Networks, Inc.

Figure 43: vGW AntiVirus Endpoint Connection Process Dialog Box



When vGW AntiVirus identifies a threat to the VM, it presents the following dialog box to inform you of it. See Figure 43 on page 71.

Figure 44: vGW AntiVirus Endpoint Threat Detection Dialog Box



Quarantined Files

When a file is quarantined as a result of an On-Access scan, the file is sequestered in the vGW Endpoint on the protected VM. The quarantined file is inaccessible by the VM, but it remains local on it. You use the Quarantine tab on the AntiVirus module to manage quarantined files. You can handle quarantined files in these ways:

- You can fetch the file. In this case, the file is hashed and transferred off the VM for further analysis.
- You can *un-quarantine* the file. In this case, the isolated file is made available again to the VM.

  In some cases, files are quarantined because of false positive results. That is, the file is suspected of being malware or infected, but that is not the case. Updating the signature database and running the scan again often resolves the problem.
- You can delete the file from the VM, if you have confirmed that it is malware or infected.

NOTE: vGW Endpoint can be used with VMware View. However, some configurations of VMware View, such as Composer, have unique configuration parameters.

For the most updated configuration information, check the JTAC Knowledge Base.

vGW Endpoint Components and Displays

The vGW Endpoint includes the following components:

- A filter driver that performs the file monitoring and scan policy enforcement.
- A service that handles communication with the vGW Security VM. It is responsible for reporting the state and enforcing the vGW AntiVirus policy, such as quarantining a file for On-Access scans.
- A tray application that reflects the known state to the service in the vGW Security Design VM. This application has three main states represented by three icons:
  - Red warning triangle—When a threat is detected, a message box appears with a red warning triangle. When the threat is dismissed, the red triangle disappears.
  - Clear burst—All components are running and connected to the vGW Security VM.
  - Burst with yellow triangle icon—The service and driver are running, but communication has not yet been fully established with the vGW Security VM.
  - Burst with red x—Either the service or the driver is not loaded. The vGW AntiVirus policy cannot be enforced in this state. When the problem is resolved, the clear burst appears.

Copyright © 2015, Juniper Networks, Inc.

vGW Endpoint Behavior

The vGW Endpoint captures file accesses and forwards them to the vGW Security VM for analysis. The vGW Endpoint driver caches the results of the scan. You cannot control how much of a file is transferred to the vGW Security Design VM. However, the file transfer, which is controlled internally, is efficient, based on its match against the AntiVirus signatures. Only as much of the file as is necessary to determine if it is malicious is forwarded.

The vGW Endpoint cache is not associated with a timer. For this reason, you cannot control when the cache is cleared. However, the cache is cleared during installation, un-installation, and reboot processes, when the AntiVirus signature set is updated, which is typically every few hours, and when there is a version change. You use the Settings module Security Settings > AV Settings page to specify the update frequency of the AntiVirus signatures.

NOTE: **Restarting the Endpoint does not clear the cache.**

Related Documentation

- Understanding vGW Series AntiVirus on page 51
- vGW AntiVirus Configuration Overview on page 58
- *Understanding and Configuring the vGW Series AntiVirus Settings*
- Configuring vGW Series AntiVirus On-Demand Scanning on page 78
- *Understanding vGW Series*
- *Understanding the vGW Security VM*

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 6

AntiVirus Scanning Config

- Configuring vGW Series AntiVirus On-Access Scanning on page 75
- Configuring vGW Series AntiVirus On-Demand Scanning on page 78

Configuring vGW Series AntiVirus On-Access Scanning

This topic explains how to configure a vGW AntiVirus On-Access scanner configuration using the AntiVirus module Scanner Config tab. The On-Access scan protects VMs against malicious content and virus infections that can occur whenever a file is read from or written to disk. If On-Access scanning is configured, vGW AntiVirus intercedes and checks the file against the signature database to ensure that the content does not contain malware or a virus. By blocking an infected file, On-Access scanning protects the network from malicious attacks at the source, before damage is done.

Before you configure a vGW AntiVirus On-Access scan, you must perform prerequisite tasks. These tasks configure other parts of the system that allow vGW AntiVirus to quarantine an entire VM with the Quarantine policy when the VM is compromised by a virus. They also initiate communication with the vGW Endpoint:

- Deploy the vGW Security VM to the ESX/ESXi hosts in your environment.
- Configure and install firewall policies on the VMs to be protected.

When you configure a custom On-Access scan, you can specify types of files and files at certain locations to be scanned, and you can exclude certain types of files and files at certain locations from the scan. You can combine these options, for example, to scan all file types but only in a certain directory or to exclude certain types of files in a certain directory.

Consider the following characteristics, when you configure custom On-Access scans:

- When specifying a file location, for On-Access scans you must always specify the drive letter.
- vGW Series does not support the use of wildcards in specifying file types or file locations.

The vGW Endpoint captures file accesses and forwards them to the vGW Security VM for analysis. The vGW Endpoint driver caches the results of the scan. You cannot control how much of a file is transferred to the vGW Security Design VM. However, the file transfer, which is controlled internally, is efficient, based on its match against the AntiVirus

Copyright © 2015, Juniper Networks, Inc.

signatures. Only as much of the file as is necessary to determine if it is malicious is forwarded.

NOTE: Because the scan is performed on the vGW Security VM, it is not necessary to re-configure a VM after an On-Access scan.

To create an On-Access vGW AntiVirus configuration or add a new one:

1. Select the AntiVirus module **Scanner Config** page.

   The AV Scanner Configuration table is displayed showing information about existing AV scanner configurations. The table shows the scanner configuration name, the scope of VMs that the scan covers, and the type of scan: On-Access, On-Demand, or both.

2. Click **Add**.

3. Specify a name for the AntiVirus scanner configuration.

4. (Optional). Give a brief description of the scanner configuration so that it is quickly recognizable.

5. In the Scope box, identify the VM groups whose VM members are to be scanned.

   For a VM to be protected by vGW AntiVirus, it must belong to a VM group that you include in the scan scope.

   To select the scope, click **Select**. A pop-up dialog box is displayed that shows all VMs groups on the left side. Click on the name of a group and move it to the **Selected Groups** section on the right. Click **Apply**.

   After a scan is defined, it is added to the list of configurations in the AV Scanner Configuration table.

   NOTE: If a VM group is a member of more than one scanner configuration, the topmost scan definition that it belongs to is used to protect it. You can manipulate the order of the scanner configurations in the table by selecting the row for the scanner configuration and clicking either **Move Up** or **Move Down**.

6. In the **Step 1 Scan Options** pane, select the **On-Access Scanning** check box. By default, both types of scans are selected. In this case, clear the check box for **On-Demand Scanning**.

   NOTE: Step 2 in the scanner configuration page is required for On-Demand scans only, so it is not included in this procedure.

Copyright © 2015, Juniper Networks, Inc.

7. In the **Step 3 Configure Scanning Engine** pane, select the type of scan to perform. Under **On-Access file types/extensions scanning selection**, select either **Typical Scan** or **Custom Scan**. For this example, select the **Typical Scan** check box.
8. In the **Step 4 Action pane**, specify one or more actions to take when the scan detects a virus:
   - **Alert when a virus is detected**—The Virus Alerts tab displays information on the VMs or files that are infected.
   - **Quarantine VM**—You can specify that the infected VM is to be included in a quarantine policy group.

     You use the Quarantine page on the Main module to view a list of VMs quarantined as a result of an AntiVirus scan. From the Main module Quarantine page, you can remove a VM from quarantine by selecting the VM and clicking **Un-Quarantine VM**.
   - **Quarantine infected files**—You can specify that infected files be quarantined.

     Use the Quarantine Files page on the AntiVirus module to display a list of files that are quarantined and take action.

     The Quarantine Files page lets you delete an infected file, remove it from quarantine, or fetch it to remediate it according to your own process.
   - **Suspend the VM**—You can suspend the VM entirely.

   Use the Quarantine Files page on the AntiVirus module to display a list of files that are quarantined and take action. See *Understanding Quarantined VMs and Files Resulting from a vGW AntiVirus On-Access Scan*.

To create a custom scan that allows you to specify the files to be scanned:

1. In the Step 3 Scan Engine Configuration pane, under the On-Access file types/extensions scanning selection, select the **Custom Scan** option button.
2. Select the files to scan.

   NOTE: **The file types and the file locations that you specify in this pane work together to clearly identify the files to scan. For example, if you select Scan All File Types and Scan Only—for example to scan only specific locations such as c:\user\share—then all the files at that location are scanned, but only those files.**

   a. Select the **Scan Archives** check box to scan all files archived in various formats.

      NOTE: **For improved performance, do not scan archive files.**

   b. Select the types of files to scan. Select one of the following options:
      - **Scan All File Types**—Scans all types of files, delimited by the selected file location.

- **Scan Only**—Scans only specified file types, delimited by the selected file locations. You can delete file types from the provided list to exclude them from the scan.
- **Ignore only**—Scans all types of files except the specified types.

c. Select the locations where the files to scan reside.

For On-Access scans, when scanning files based on location, vGW Series takes into account the drive letter of the directory. For example, given the file location C:\Program, an On-Access scan scans files only in that directory. It does not scan files in the D:\Program directory, although the directory names are the same, because it acknowledges that the drive letters are different. You must specify the drive when you specify the location of files to scan for custom On-Access scans.

- **Scan All Locations**—Scans files in all locations, delimited by the selected types of files to scan.
- **Scan only**—Scans files only at the specified location, delimited by the selected types of files to scan.
- **Ignore only**—Scans all files except those that reside at the specified locations.

Related Documentation

- Understanding vGW Series AntiVirus on page 51
- vGW AntiVirus Configuration Overview on page 58
- Understanding and Installing the vGW Endpoint on page 69
- *Understanding and Configuring the vGW Series AntiVirus Settings*
- Configuring vGW Series AntiVirus On-Demand Scanning on page 78
- *Understanding vGW Series*
- *Understanding the vGW Security VM*

Configuring vGW Series AntiVirus On-Demand Scanning

This topic explains how to configure the On-Demand vGW AntiVirus scan feature that allows you to schedule an offline full disk scan. For a smaller scan footprint, you can identify the parts of your disk that you want scanned, or you can exclude parts of it from the overall scan. To gain an overall understanding of AntiVirus configuration, before you read this topic, read "vGW AntiVirus Configuration Overview" on page 58.

NOTE: **On-Demand scans are performed without any impact to the VM. The scanning is done outside the VM on the ESX/ESXi host's vGW Security VM. Therefore it not necessary to re-configure a VM after an On-Demand scan.**

On-Demand scanning does not require that any software be installed in the VM. That is, you do not need to install the vGW Endpoint, which is required for On-Access scans.

On-Demand scanning can be used for many purposes. Some companies run On-Demand scans regularly to check for compliance. Public clouds that host many customer VMs

 Copyright © 2015, Juniper Networks, Inc.

but that do not have jurisdiction to install vGW Endpoints on the VMs use On-Demand AntiVirus scanning.

NOTE: **You can configure both On-Access Scanning and On-Demand Scanning in a single AntiVirus configuration.**

The On-Demand scanner performs rootkit detection. The vGW AntiVirus engine contains signatures that help to identify rootkit files. It can detect files with suspicious names such as mal.exe, and simpletroj.exe. Because you do not need to protect VMs with the vGW firewall and you do not need to install the vGW Endpoint on the VM, On-Demand scans can be performed on virtual disk files from a protected location that is not compromised. This advantage increases the ability of vGW AntiVirus to detect and locate rootkits. The vGW AntiVirus engine contains signatures that help to identify rootkit files. It can detect files with suspicious names such as mal.exe, simpletroj.exe, and so on.

vGW Series scans one VM at a time to avoid problems such as brown-outs that could ensue during an On-Demand full disk scan if all VMs were scanned concurrently. The entire disk is scanned according to the schedule configuration specifications, but VMs are scanned sequentially. This approach applies also to custom scans in which only selected areas of a disk are scanned.

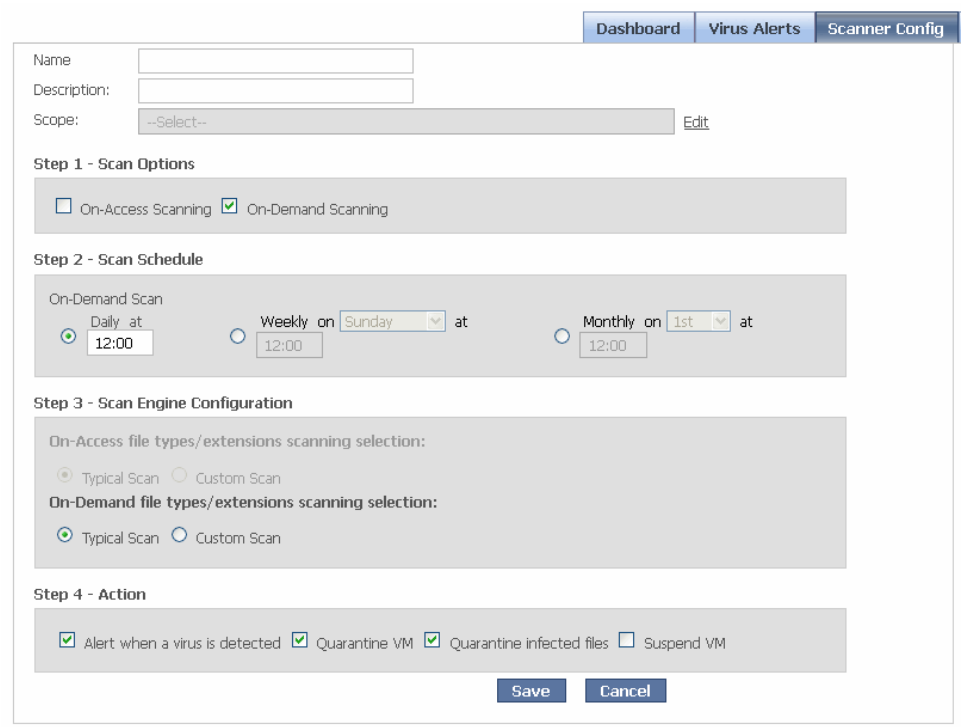
For On-Demand scans, vGW Series scans 500 MB per second. To gain an understanding of how long a disk scan takes, consider the following equation:

<*VM memory size*> x < *number of VMs on disk*> / 500 MB per second

To create an On-Demand vGW AntiVirus configuration or add a new one:

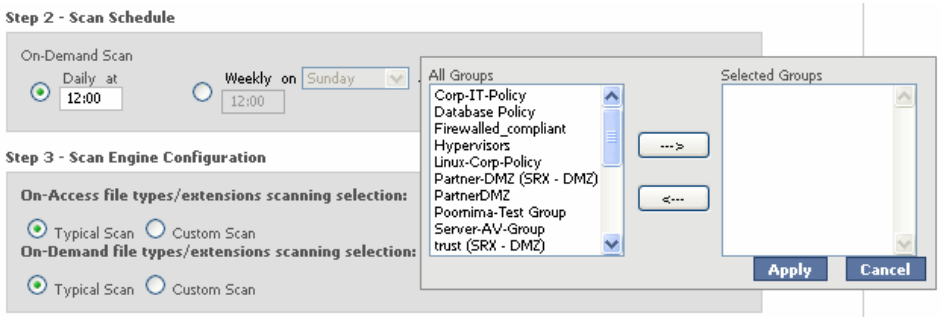
1. Select the vGW AntiVirus module. On the main vGW AntiVirus page, select the **Scanner Config** tab, and click **Add**. Figure 45 on page 80 shows the configuration page that appears.

Figure 45: Scanner Config Tab



2. Specify a name for the vGW AntiVirus On-Demand configuration scan.
3. Select the **On-Demand Scanning** option button.
4. (Optional) Give a brief description of the configuration so that it is quickly recognizable.
5. From the All Groups list in the **Scope** box, identify the VM groups to be scanned. See Figure 46 on page 80.

Figure 46: Step 2: Scan Schedule

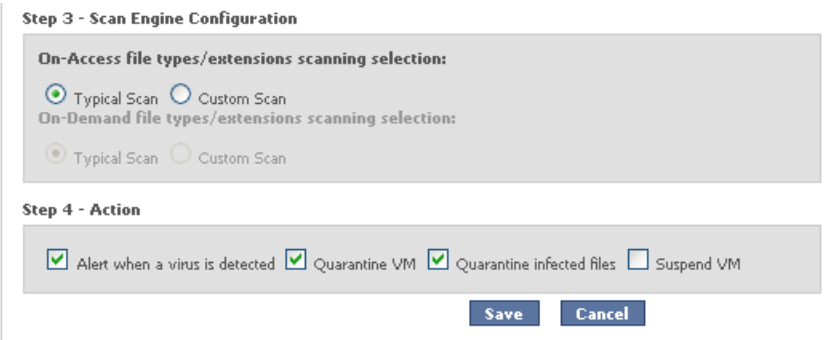


Copyright © 2015, Juniper Networks, Inc.

6. In the Step 2 Scan Schedule pane, specify when you want the vGW Series to perform the scan.

   You can schedule daily, weekly, or monthly scans.

7. In the Step 3 Scan Engine Configuration pane, select the type of scan to perform, either Typical Scan or Custom Scan. For this example, select the **Typical Scan** option button.



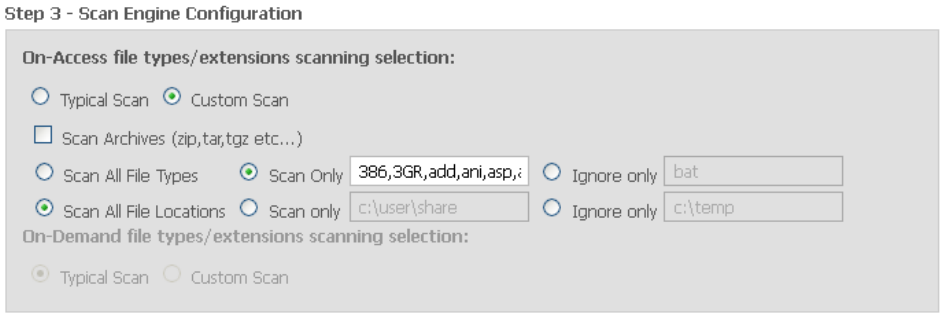
8. In the Step 4 Action pane, specify the action to take when the scan detects a virus:

   CAUTION: **For On-Demand scans, you cannot quarantine files or VMs.**

   - **Alert when a virus is detected**—The Virus Alerts tab displays information on the VMs or files that are infected.
   - **Suspend the VM**—You can suspend the VM entirely.

To create a custom scan that allows you to specify the files to be scanned:

1. In the Step 3 Scan Engine Configuration pane, under the On-Demand file types/extensions scanning selection, select the **Custom Scan** option button.



2. Select the files to scan.

   The file types and the file locations that you specify in this section work together to clearly identify the files to scan. For example, if you select **Scan All File Types** and **Scan Only** (specified locations, for example c:\user\share), then all the files at that location are scanned, but only those files.

Take into account the following characteristics when you configure a custom On-Demand scan:

- vGW Series recognizes the global wildcards * and ?.

  For example, you could specify C:\Program Files\MS*. You could also use the wildcard on an extension, for example doc*.

- For file locations, drive letters are ignored. For example, C:\Program Files matches the following directories, and files in both these locations are scanned:

  C:\Program Files and D:\Program

  vGW Series performs an On-Demand scan offline and does not take into account drive letters.

Select the **Scan Archives** check box to scan all files archived in various formats. For improved performance, do not scan archive files.

3. Select the types of files to scan. Select one of the following:
   - **Scan All File Types**—Scans all types of files, delimited by the selected file location.
   - **Scan Only**—Scans only specified file types, delimited by the selected file location. You can delete file types from the provided list to exclude them from the scan.
   - **Ignore only**—Scans all types of files except the specified types.
4. Select the locations where the files to scan reside.
   - **Scan All Locations**—Scans files in all locations, delimited by the selected types of files to scan.
   - **Scan only**—Scans files only at the specified location, delimited by the selected types of files to scan.
   - **Ignore only**—Scans all files except those that reside at the specified locations.

Related Documentation

- Understanding vGW Series AntiVirus on page 51
- Understanding and Installing the vGW Endpoint on page 69
- *Understanding and Configuring the vGW Series AntiVirus Settings*
- Configuring vGW Series AntiVirus On-Access Scanning on page 75
- *Understanding vGW Series*
- *Understanding the vGW Security VM*

Copyright © 2015, Juniper Networks, Inc.

PART 3

Introspection

- Introspection Module Basics on page 85
- Introspection Software Monitoring on page 87
- Image Enforcer and Enforcer Profiles on page 93
- Scans and Scheduling Scans on page 101
- Registry Inspection on page 105

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 7

Introspection Module Basics

- Understanding the vGW Series Introspection Module on page 85

Understanding the vGW Series Introspection Module

The vGW Security Design VM Introspection module lets you monitor the software installed on guest virtual machines (VMs) in your virtual infrastructure. You can monitor software that is installed on all MS Windows VMs and some Linux VMs that support the RPM package manager when the system scans for installed applications. Without installing endpoint software in the guest VMs, vGW Series can determine which applications are installed, the operating system type (for example, for MS Windows, XP, 2003, and so on), and it can identify registry values and any applied updates (hotfixes).

NOTE: **Because not all Linux VMs support RPM, we recommend that you refer to the Juniper JTAC Knowledge Base for the most current information.**

When the system scans for installed applications on MS Windows VMs, it also scans registry information. Mostly the vGW Security VM performs the scans.

For Introspection, the vGW Series centralizes the scanning engine to limit disk IO, memory, and CPU consumption, and to distribute the load across responsible vGW Security VMs. Because vGW Security VMs are responsible for most of the scanning, scalability concerns are lessened, the process is faster, and introduction of new security risks is avoided. Although most of the scanning is constrained to vGW Security VMs, both the vGW Security VM and the vGW Security Design VM engage in the process. That is, by default the scan is performed by the vGW Security VM, but it is possible to scan a VM on which the vGW Security VM is not installed. The scan can be performed by the vGW Security Design VM.

WARNING: **TCP Port 902 must be open between the vGW Security Design VM and the ESX/ESXi hosts for Introspection to work properly if the vGW Security Design VM is performing it.**

The Introspection module relies on taking a snapshot of a VM and analyzing it. This method guarantees that there is no adverse impact on the active VM during the scan. After the scan is complete, the snapshot is deleted immediately. The Introspection feature

Copyright © 2015, Juniper Networks, Inc.

is supported in both IPv4 and IPv6 environments. vGW Series can mount disks that belong to VMs with either an IPv6 address or IPv4 address bound to them.

The scan does not use network packets to probe applications in the VM. Rather, it uses native VMware interfaces to examine the disk contents. This enables a fast and accurate scan. It takes only a few seconds for vGW Series to analyze the installed applications.

The ability to determine exactly which applications are installed allows the security policy for those VMs to be precise and dynamically applied. For example, you can analyze the VMs to determine which ones are running the Apache Web server. You can then place those VMs in a Smart Group and give it a name such as "webservers". You can configure this Smart group with a policy that allows communication through HTTP/HTTPS.

The Introspection module makes it possible for you to assess applications that are installed in the environment that are secured and those that are required but are missing. For example, you can quickly identify VMs that do not have an vGW Endpoint, if the Endpoint is required. You can quarantine these VMs with a restrictive firewall policy.

Although the Introspection feature is not intended to replace a patch management solution, you can use its capabilities in this area to determine if certain hotfixes are missing. You can then quarantine the hosts without the required hotfixes until the patch management solution deploys the proper updates.

The vGW Security Design VM groups the introspection results by type (application, operating system, and hotfix). It provides graphical summary comparisons and detailed statistics about the installed software in table format.

The Introspection page includes the following tabs:

- Applications

  For details, see "Understanding the vGW Series Introspection Applications Tab" on page 87.

- VMs

  For details, see "Understanding the vGW Series Introspection VMs Tab" on page 90.

- Enforcer Profiles

  For details, see "Understanding the vGW Series Enforcer Profiles Tab" on page 95.

- Scan Status

  For details, see "Understanding the vGW Series Introspection Scan Status" on page 102.

- Scheduling

  For details, see "Understanding the vGW Series Introspection Scheduling Feature" on page 101.

Related Documentation

- *Understanding vGW Series*

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 8

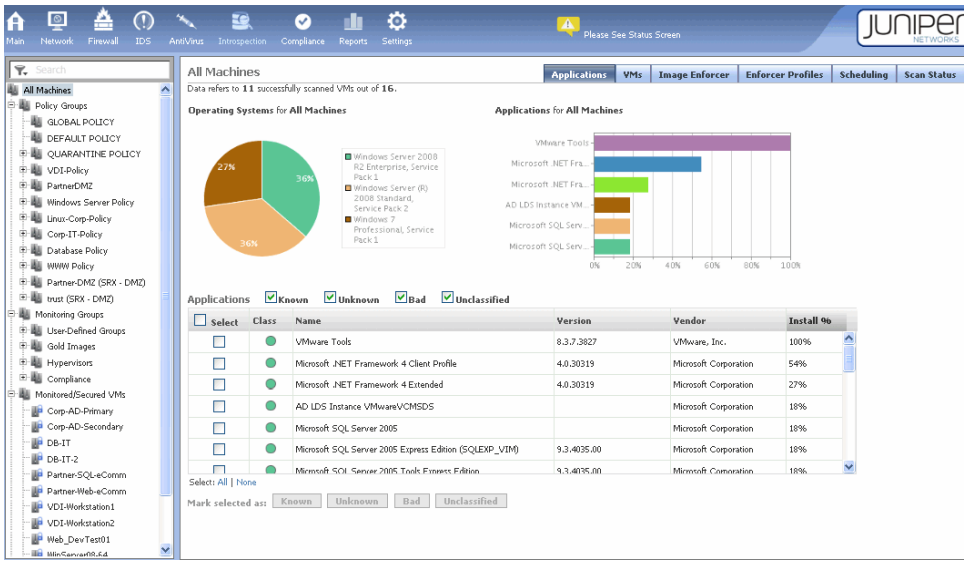
Introspection Software Monitoring

- Understanding the vGW Series Introspection Applications Tab on page 87
- Understanding the vGW Series Introspection VMs Tab on page 90

Understanding the vGW Series Introspection Applications Tab

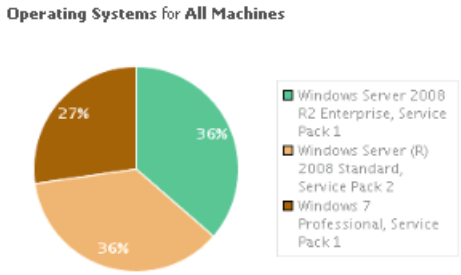
The Introspection module of the vGW Security Design VM includes an Applications tab that displays the following information about software currently installed on guest virtual machines (VMs). You select the VMs in the VM Tree that you want to inspect.

Figure 47: vGW Series Introspection Module Applications Tab

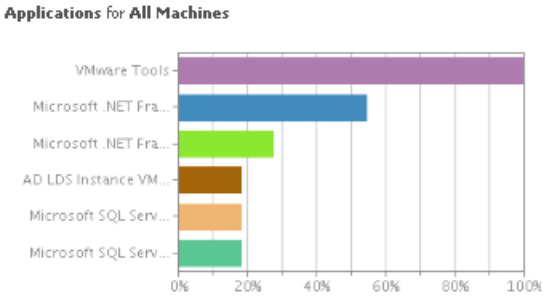


The Applications tab contains:

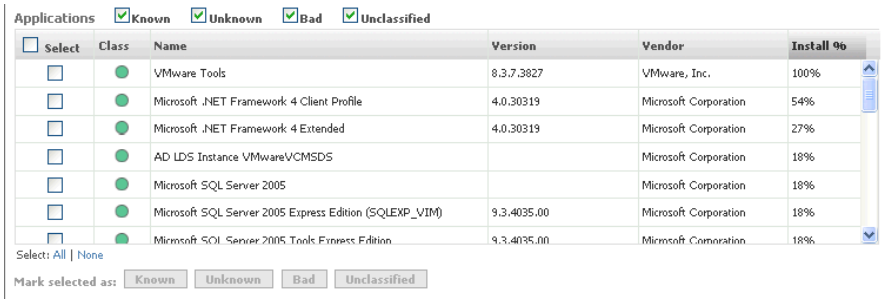
- A pie chart comparing the percentage of each type of operating system running across all secured VMs.



- A bar graph comparing the percentage of each type of application installed on all secured VMs.



- A detailed list of each application. You can control which types of applications are included. For example, you can select only **Bad** to list applications that should not be installed on secured VMs.



NOTE: If you select a group of VMs in the VM Tree, the vGW Series summarizes the data in pie and bar charts. If you select a single VM, you can view detailed information in table format.

You use the Applications tab:

- To discover information about the software installed in your environment. It provides:

Copyright © 2015, Juniper Networks, Inc.

  - A quick overall software assessment. It allows you to quickly determine the types of installed software without regard to the exact VMs that contain it.
  - The percentage of VMs running particular software. You can use this tab when you want to determine the percentage of VMs in your environment that are running a particular application, service pack, or operating system.
  - Information specific to a VM or VM group. You can use this tab to discover which applications are installed on VMs or groups of VMs.

- To categorize the software installed throughout your environment. This classification system allows you to monitor the VM software state to determine if any VMs are running unauthorized or inappropriate software based on your specifications.

  You can select one or more applications in the table and mark them with one of the following classifications:

  - **Known**—Use this classification for applications that are acceptable for your virtualized environment.
  - **Unknown**—Use this classification when an application is present, but you are unsure if it is appropriate for the environment.
  - **Bad**—Use this classification for applications that are unacceptable for and prohibited from your environment.
  - **Unclassified**—Use this classification when you have not yet examined an application. Newly installed applications initially show up as Unclassified.

To control displayed information:

- Click **Select All** to select all applications running in the selected VMs.
- Select **None** to clear all selected applications.
- Click a column heading in the table to sort applications by name or vendor.

The applications bar graph updates automatically as you change your selections.

Related Documentation

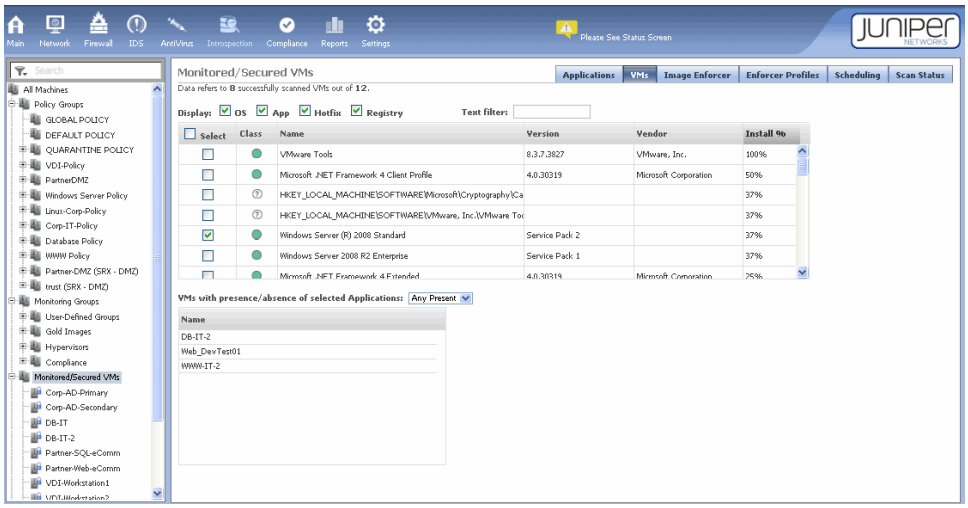
- Understanding the vGW Series Introspection Module on page 85
- Understanding the vGW Series Introspection VMs Tab on page 90
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Registry Check Feature on page 105
- Understanding the vGW Series Image Enforcer Tab on page 94
- Understanding the vGW Series Introspection Image Enforcer Feature on page 93
- *Understanding vGW Series*

Understanding the vGW Series Introspection VMs Tab

The vGW Security Design VM Introspection feature VMs tab lets you monitor software installed on a selected VM or on a group of VMs. You can display or hide information about the operating system and about applications running on the VM, including details about installed service packs and hotfixes. You can use this feature to determine if software is present or absent on one or more VMs. The VMs tab is useful in determining which VMs have certain types of software installed.

In Figure 48 on page 90, VMs in the User-Defined Groups which is selected in the VM tree are scanned to determine if they contain the Microsoft .NET Framework 4 Client Profile.

Figure 48: vGW Series Introspection Module VMs Tab



There are many ways to use this feature. For example, you can

- view all VMs that are running the MS Windows Server 2003 operating system, or all VMs that have a specific hotfix installed.
- determine the VMs that are running a specific application, such as Kazaa or Skype.
- discover VMs that are missing required software.

To search for a specific item in the list by name or vendor, click the **Name** or **Vendor** column heading in the details table, and then type the name of the software or vendor in the **Text** filter box. The list refreshes to show entries that match your specification.

You can also search the VMs to discover those that contain specific software and then filter based on a group setting in the VM Tree. To do so, select the group in the VM Tree, and then select one or more types of software in the table.

For example, select the **filter VMs with presence/absence of select Applications**, and then choose **All Present**, **Any Present**, **All Absent**, **Any Absent** from the menu. A list of VMs meeting your criteria appears in the lower table.

Copyright © 2015, Juniper Networks, Inc.

vGW Series Introspection feature can discover installed software regardless of firewall settings. Because vGW Security VMs are responsible for most of the scanning, Introspection does rely on the vGW Security Design VM. That is, by default the scan is performed by the vGW Security VM. However, it is possible to scan a VM on which the vGW Security VM is not installed. In this case, the scan can be performed by the vGW Security Design VM.

WARNING: **TCP Port 902 must be open between the vGW Security Design VM and the ESX/ESXi hosts for Introspection to work properly if the vGW Security Design VM is performing it.**

Related Documentation

- Understanding the vGW Series Introspection Module on page 85
- Understanding the vGW Series Introspection Applications Tab on page 87
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Registry Check Feature on page 105
- Understanding the vGW Series Image Enforcer Tab on page 94
- *Understanding vGW Series*
- Understanding the vGW Series Introspection Image Enforcer Feature on page 93

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 9

Image Enforcer and Enforcer Profiles

- Understanding the vGW Series Introspection Image Enforcer Feature on page 93
- Understanding the vGW Series Image Enforcer Tab on page 94
- Understanding the vGW Series Enforcer Profiles Tab on page 95

Understanding the vGW Series Introspection Image Enforcer Feature

The vGW Security Design VM Introspection module provides a constellation of information that allows you to monitor the software installed in MS Windows and Linux guest virtual machines (VMs). It gives you deep knowledge into the state of a VM and the applications flowing between VMs, and how they are used. It can tell you the operating system versions and the services patches versions that are installed on VMs. It presents this information about the installed software to you through graphical summary comparisons and detailed statistics in table format. To facilitate management of this large amount of information and to enable you to pro-actively classify applications, the vGW Series provides an Introspection feature called the Image Enforcer.

Central to the Image Enforcer feature is the concept of a Gold Image. A Gold Image is a template from which VMs are derived, but it can also be an active VM. The Gold Image template or VM candidate has a valid and desirable configuration. When it is identified as a Gold Image, the VM is elevated to the level of a model VM configuration.

You use the Enforcer Profiles tab to create a profile for a Gold Image. In the profile, you also specify the VMs to be compared against the Gold Image and parameters that qualify the comparison. You can allow VMs to deviate from the Gold Image in various ways.

When a template is used as a Gold Image, usually the VMs that are derived from it are compared against it. For example, you might want to determine how much and in what ways their configurations have been changed since they were instantiated from the template. However, you can specify any VMs to compare against a Gold Image, not only those that were derived from it.

You can direct the vGW Security Design VM to take certain actions based on the outcome of the comparison. For example, you can direct it to quarantine noncompliant VMs. VMs that are quarantined are viewable in the Image Enforcer page and the Main module's Quarantine page. From the Quarantine page, you can release a quarantined VM, for example, and modify it to reinstate it as a valid VM or to perform other kinds of

Copyright © 2015, Juniper Networks, Inc.

remediation. For details on the Main module's Quarantine tab, see *Understanding the vGW Series Main Module*.

You can use the Image Enforcer tab to view a summary of the comparison results and gain an overall sense of the compared VMs' conformance to the Gold Image. You can also view a bar graph specific to a particular VM to see the degree to which it conforms.

There are many ways in which to use the Image Enforcer feature:

- You might create a SQL Servers Gold Image to check for noncompliant servers.
- You might create a Desktops Gold Image and compare desktop software against it.

Consider another case. Suppose you want to use a template whose configuration is approved by auditors for PCI compliance as a Gold Image and call that Gold Image PCI-Win-Template. You could then compare the VMs belonging to the Win-PCI-Servers and PCI-Desktop VMs groups against the PCI-Win-Template Gold Image. As part of the comparison criteria, you might specify that applications classified as "known" are allowed. Although the Gold Image configuration does not contain them, a VM whose configuration contains these known applications would not be considered non-compliant.

vGW Series automatically creates a compliance rule for each Gold Image that is a template. By default, it inspects the VMs derived from the Gold Image, and it generates an alert when the compliance state changes.

You can specify when the vGW Series should scan the VMs. You can set up a scan to take place when specific events occur or based on a defined schedule that you create using the Scheduling tab. You can also limit the number of concurrent scans.

Related Documentation

- Understanding the vGW Series Introspection Module on page 85
- Understanding the vGW Series Introspection Applications Tab on page 87
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Registry Check Feature on page 105
- Understanding the vGW Series Image Enforcer Tab on page 94
- *Understanding vGW Series*

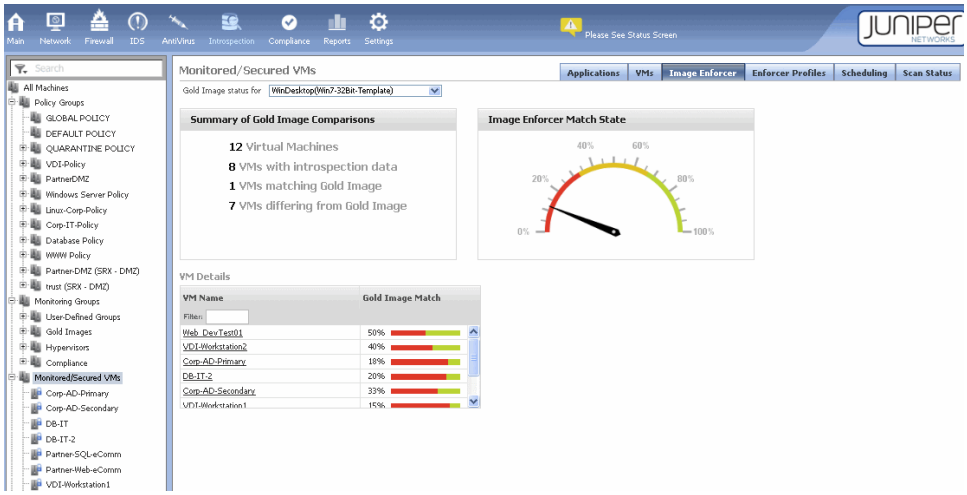
Understanding the vGW Series Image Enforcer Tab

The Introspection module's Image Enforcer tab reports on results of comparisons between guest virtual machines (VMs) and model templates or active VMs that are referred to as Gold Images.

Figure 49 on page 95 shows the Image Enforcer tab page displaying results of a scan in which VMs that belong to the Monitored/Secured VMs group are compared to the WinDesktop(Win7-32bit-Template) Gold Image. The groups that are included in the scan are selected in the VM tree.

 Copyright © 2015, Juniper Networks, Inc.

Figure 49: vGW Series Introspection Module Image Enforcer Tab



The Image Enforcer tab page shows the following results of a comparison:

- It identifies matches. That is, it identifies software installed on a VM that is also installed on the Gold Image.
- It identifies applications that are installed on a VM that are not installed on the Gold Image.
- It identifies applications installed on the Gold Image that are not installed on a VM.
- It checks software versions, and it identifies versions on VMs that do not match those of the Gold Image.

Related Documentation

- Understanding the vGW Series Introspection Module on page 85
- Understanding the vGW Series Introspection Applications Tab on page 87
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Registry Check Feature on page 105
- *Understanding vGW Series*

Understanding the vGW Series Enforcer Profiles Tab

This topic describes the vGW Series Introspection module's Enforcer Profiles tab. It explains how to use the Enforcer Profiles page to create profiles that allow you to compare the configurations of VMs to that of a Gold Image. It covers the information that you select or specify to create or modify a profile.

The Image Enforcer allows you to compare VMs to a VM template or an active VM that is elevated to the status of a Gold Image. For a template or an active VM to be considered a Gold Image, Gold Images are VM templates or VMs whose configurations are considered valid and desirable. Based on the outcome of the comparison scan, you can take actions

such as quarantining VMs that deviate from the Gold Image, or adding or removing applications from a VM to bring it into conformance.

When VMs are quarantined, they are added to the Quarantine Policy Group. When you select a quarantined VM that is in the group, the Main module dashboard is displayed, showing compliance status for the VM, its top talkers, and IDS alerts for it. You can select the Main module Quarantine tab to take action on the VM. The Main module Quarantine tab displays information about VMs that have been quarantined as a result of AntiVirus, Compliance, or Image Enforcer scans. Using it, you can view the time that the VM was quarantined, when it was removed from quarantine, and the reason that it was quarantined.

Before you read this topic, read "Understanding the vGW Series Introspection Image Enforcer Feature" on page 93.

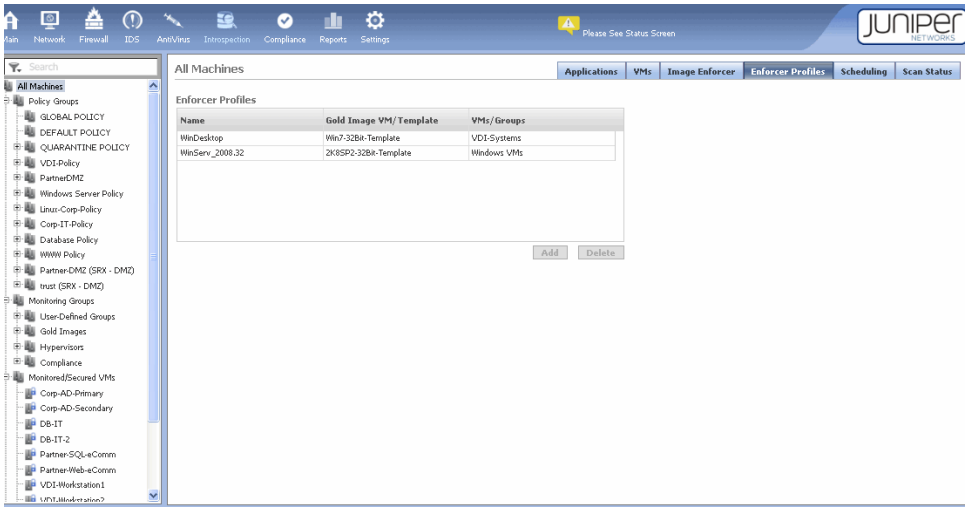
This topic includes the following sections:

- About the Enforcer Profiles Screen on page 96
- The Add Enforcer Profile Pane on page 96

About the Enforcer Profiles Screen

When you select the Introspection module Enforcer Profiles tab, the Enforcer Profiles page is displayed. Information shown in this page reflects the profiles that you have already configured, if any. You add a new Enforcer Profile from this page.

Figure 50: vGW Series Introspection Module Enforcer Profiles Tab



When you add a new profile, you give it a name that then appears in the profiles list. For each profile, the list shows the Gold Image that you selected for it and the VMs compared against it.

The Add Enforcer Profile Pane

To add a new profile, click **Add** beneath the Enforcer Profiles pane. The Add Enforcer Profile pane appears. You use this pane to configure Enforcer profiles that cover

Copyright © 2015, Juniper Networks, Inc.

parameters for a comparison scan. In this pane, you select the Gold Image to use for the comparison; you can specify match criteria to define the comparison; and you can specify actions to take after the scan completes. You can specify conditions that exempt VMs from certain requirements, and you can specify whether the vGW Security Design VM should quarantine a non-complaint VM.

Figure 51: Adding a vGW Series Introspection Module Image Enforcer Profile

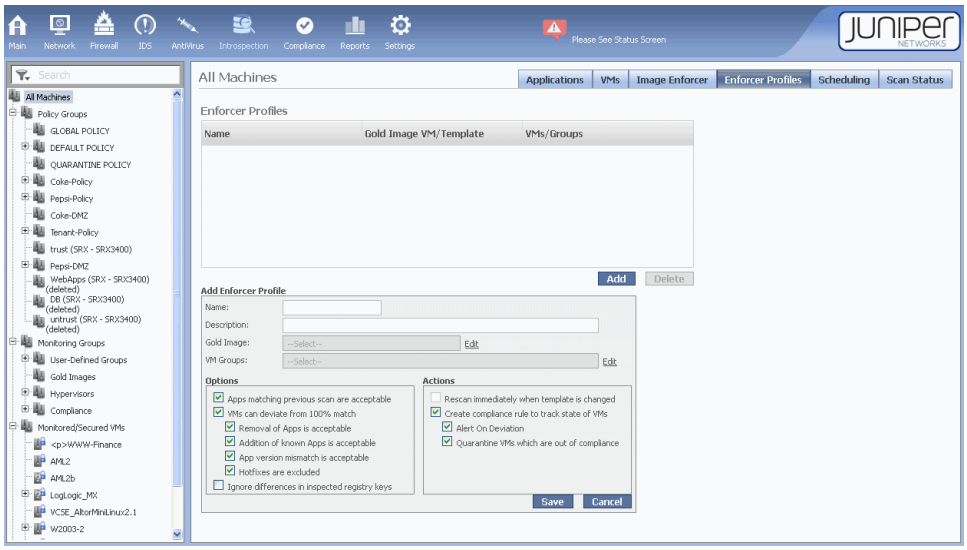


Table 6: Add Enforcer Profile: Selecting the Gold Image and VMs to Be Compared Against It

Field	Specifies
Name	A name for the profile that infers its contents.
Description	A description of the profile that indicates what it is used for.
Gold Image	The VM template or VM to use as the Gold Image for this comparison. You use the Gold Image selection list to select either an existing template or VM. Using the option button at the bottom of the selection list, you can choose to see all Gold Image candidates or only templates or VMs. NOTE: After you elevate a template or VM to the status of a Gold Image, it is moved to the Gold Images group in the Monitoring Group section of the VM tree.
VM Groups	The VM groups or VMs whose configurations you want to compare against the selected Gold Image. Use the arrow buttons to include or remove a VM group or VM from the profile.

Table 7: Edit Enforcer Profile Options

Option	If you select this check box, you specify that
Apps matching previous scan are acceptable	If a VM was previously scanned against the profile's Gold Image and matched it, but it no longer does, the VM is allowed. In this case, a Gold Image might have been updated and re-scanned. Because it takes time to update the VMs specified in the Enforcer Profile group, they are allowed as matching during the transition.
VMs can deviate from 100% match	A VM compared against the profile's Gold Image is allowed to deviate from it in any of the ways that you specify by selecting options identified in Table 8 on page 98.
Ignore differences in inspected registry keys	You permit differences in registry key application settings from those of the Gold Image.

Table 8: VM Gold Image Allowed Deviations

Option	If you select this checkbox, you specify that:
Removal of apps is acceptable	An application that is missing from the VM, but that is present on the Gold Image is acceptable.
Additions of known apps is acceptable	If an application is part of a Gold Image, it is classified as known.
App version mismatch is acceptable	The VM can contain an older or more recent version of an application than the one that exists on the Gold Image.
Hot fixes are excluded	Hot fixes are exempted from the comparison and are allowed on the VM.

CAUTION: Although you select the "App version mismatch is acceptable" option to allow a VM to contain an older or more recent version of an application than the one that exists on the Gold Image, the option might not take effect. For example, an application might have a version number as part of its program name on the MS Windows control panel. In this case, the version number might not be recognized and vGW Series would not allow the deviation. The actions that you specify in the Actions section of the Add Enforcer pane would be enacted on the VM.

Table 9 on page 99 identifies the actions that you can direct vGW Series to take following a comparison scan.

Copyright © 2015, Juniper Networks, Inc.

Table 9: Actions

option button	If you select this check box, you direct vGW Series to . . .
Rescan immediately when template is changed	Automatically run the comparison of the VM against the Gold Image again whenever a template that is used as a Gold Image is changed by being converted to a VM, modified, and then converted back to a template.
Create compliance rule to track state of VMs	Automatically define a compliance rule derived from the Gold Image configuration and take the actions that you select in Table 10 on page 99.

Table 10: Compliance Rule Specifications

Alert On Deviation	Notify you when the VM deviates from the Gold Image.
Quarantine VMs which are out of compliance	Quarantine VMs whose configurations do not conform with that of the Gold Image, taking into account the allowances that you specify as options described in Table 8 on page 98.

Related Documentation

- Understanding the vGW Series Introspection Module on page 85
- Understanding the vGW Series Introspection Applications Tab on page 87
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Registry Check Feature on page 105
- *Understanding vGW Series*

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 10

Scans and Scheduling Scans

- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102

Understanding the vGW Series Introspection Scheduling Feature

The Introspection module Scheduling page allows you to define schedules specifying when VMs are to be scanned.

To improve performance during peak periods, you can limit the number of concurrent scans by making a selection in the Max number of concurrent scans menu. We recommend running no more than two concurrent scans.

To define a scan schedule, click **Add**, select options for the scan, and then click **Save**. shows the Scheduling page with the Add Schedule dialog box displayed.

Figure 52: Introspection Module Scheduling Page

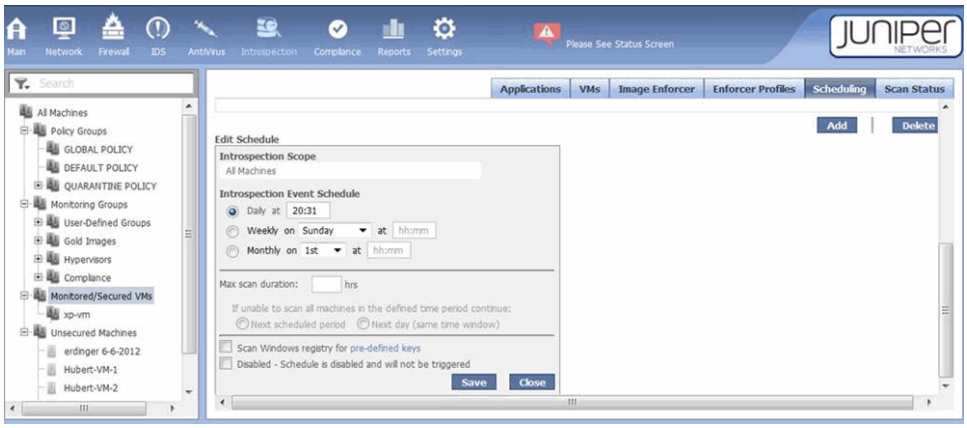


Table 11 on page 101 defines use of the fields and options.

Table 11: Scan Definition Options

Option	Select or Enter
Introspection Scope	**All Machines** or **Selected Group**, and then choose a group from the list.

Table 11: Scan Definition Options *(continued)*

Option	Select or Enter
Introspection Event Schedule	**Daily**, and then enter the hour and minute when you want the scan to begin. **Weekly**, and then select the day of the week and enter the hour and minute when you want the scan to begin. **Monthly**, and then choose day of the month and enter the hour and minute you want the scan to begin.
Max scan duration	The length of time that the scan must not exceed. You can use the **max scan duration** option to ensure that no scans occur outside maintenance. vGW Series completes a scan in progress, but it will not begin subsequent scans in the list. Any pending scans are listed in the Scan Status tab. They resume when the next scheduled time occurs.
If unable to scan...	Next scheduled period. The scan will continue at the next scheduled interval. Next day. The scan is continued at the same time tomorrow.
Scan Windows registry for pre-defined keys	Select the check box to direct vGW Series to Inspect the registry in Microsoft OS VMs to identify user-defined registry keys and their values.
Disabled – Schedule is disabled and will not be triggered	Select the check box to disable the scan disk task in the presently defined schedule. The scan will not be performed. TIP: You can use this parameter to temporarily suspend scans from occurring without your having to delete the schedule then recreate it.

To delete a schedule, select the schedule in the list and click **Delete**.

Related Documentation

- Understanding the vGW Series Introspection Module on page 85
- Understanding the vGW Series Introspection Applications Tab on page 87
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Registry Check Feature on page 105
- *Understanding vGW Series*

Understanding the vGW Series Introspection Scan Status

The Introspection Scan Status tab in the vGW Security Design VM lets you run and monitor disk scans of one or more VMs. vGW Series performs a full analysis of the selected VM's disk. If multiple disks exist in the VM system, each is analyzed. This analysis uncovers installed applications, the operating system, and the service pack/patch level running on the VM. You can select more than one VM in the VM tree to scan.

You can display current information about all scans (those complete and those still pending) or only complete or pending scans. You can also run scans manually or cancel scans in progress.

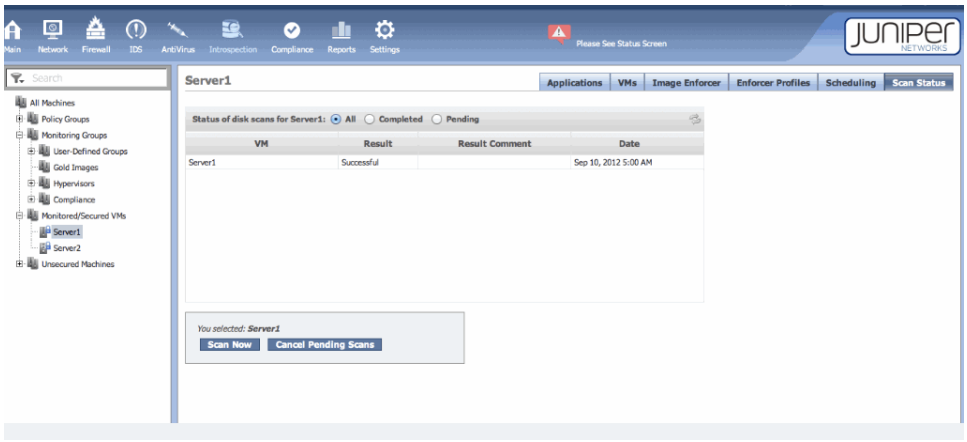
 Copyright © 2015, Juniper Networks, Inc.

To use the Scan Status page:

- To run a scan on a selected VM or group of VMs, select the VM or VMs in the VM tree, and click **Scan Now**.
- To cancel a scan in progress, click **Cancel Pending Scans**.
- To view scan results, select **All**, **Completed**, or **Pending** to control the displayed information.

Figure 53 on page 103 shows the Introspection module Scan Status page displaying the results of scans for Server1. Only one scan had been performed. The table would show the results of all scans on Server1 if any others had been run because the All option is selected.

Figure 53: vGW Series Introspection Module Scan Status Page



vGW Series scan technology is highly accurate. Rather than a network probe, vGW Series performs an actual read of the disk file from the hypervisor. The scan process is also very fast. A typical VM scan takes less than 5 minutes.

Because scanning activity takes place on a snapshot of the system, it has no impact on the operational state of the VM. When the scan has completed, the snapshot is removed.

NOTE: vGW Series can mount disks that belong to VMs that have either IPv4 or an IPv6 address bound to them.

Related Documentation

- Understanding the vGW Series Introspection Registry Check Feature on page 105
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Image Enforcer Feature on page 93
- Understanding the vGW Series Introspection Applications Tab on page 87

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 11

Registry Inspection

- Understanding the vGW Series Introspection Registry Check Feature on page 105
- Configuring the vGW Series Introspection Registry Feature on page 106

Understanding the vGW Series Introspection Registry Check Feature

You can use the vGW Security Design VM Introspection module to inspect the registry in Microsoft OS VMs to identify user-defined registry keys and their values. You can also use it to add new registry keys.

Before you use the Settings module vGW Application Settings > Registry Values page to configure the registry introspection settings, you must be familiar with the Introspection module. For details, see "Understanding the vGW Series Introspection Module" on page 85 and in particular the other topics identified in the Related Topics section of this topic.

The vGW Security VM performs the Registry inspection. It requires that the scanned VM is on a host on which the vGW Security VM resides and therefore is secured by vGW Series. However, the VM to be scanned does not need to be secured.

You can use the registry introspection feature to:

- Identify application configuration attributes. For example, it can determine if a critical directory is configured for protection by a disk encryption application.
- Validate configuration versions, such as the signature version for a DLP application in a guest VM.
- Use a registry key as internal tag to identify an MS Windows build or as an identifier for security policy automation.

You can populate the registry with values that can be used in Smart Groups for disk introspection. To configure registry introspection settings, you use the Settings module vGW Application Settings > Registry Values page. The configuration elements correlate to the registry values shown in regedit. The configuration values are:

- Name—name that identifies the registry value within vGW management.
- Key—Registry key path. Registry key names can be identified using regedit within MS Windows.
- Data—The data field contains the content associated with the chosen registry Name.

Copyright © 2015, Juniper Networks, Inc.

WARNING: The Key that you enter must begin with the prefix HKEY_LOCAL_MACHINE\. This is the only registry root that vGW Security VM currently supports. If the key that you enter does not contain this prefix, vGW Series displays the following alert message and highlights the Key input field.

Currently only registry values under root HKEY_LOCAL_MACHINE are supported. Please enter a key that starts with HKEY_LOCAL_MACHINE.

To add a new value:

1. Click **Add**.
2. Enter a Name for the configuration. For this example, enter **Sample Directory**.
3. Enter the registry Key. For this example, enter **HKEY_LOCAL_MACHINE\Software\Software\Sample Application\Sample Version**.
4. Enter a Value Name. For example, enter **SampleDir**.
5. Enter Data to associate with the registry key name. For example, enter **C:\Program Files\Sample Vendor\Sample**.
6. Click **Save**.

Related Documentation

- Configuring the vGW Series Introspection Registry Feature on page 106
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Image Enforcer Feature on page 93
- Understanding the vGW Series Introspection Applications Tab on page 87
- *Understanding vGW Series*
- Understanding the vGW Series Introspection Module on page 85

Configuring the vGW Series Introspection Registry Feature

The Security Design VM Introspection > Settings > vGW Application Settings > Registry Values feature includes a disk introspection enhancement that allows you to populate a value in the registry that you can then use in Compliance inspections and in Smart Groups. The Registry Values page displays a list of registry values that are scanned on VMs during the inspection process.

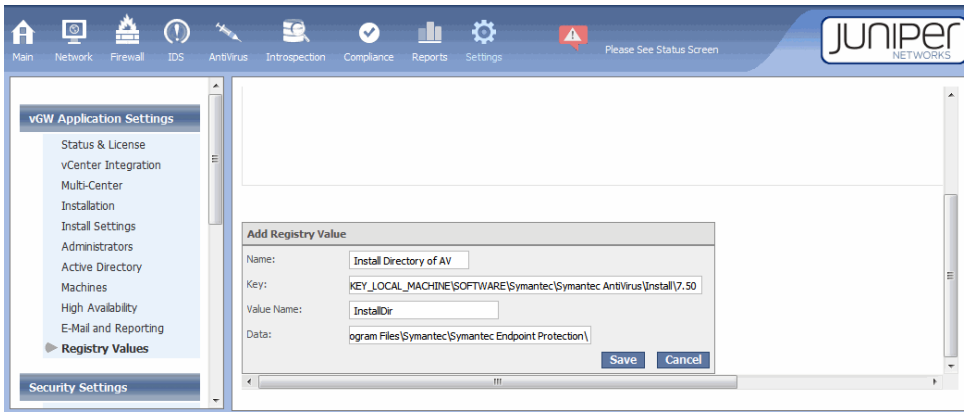
Before you use the Registry Values page to configure the registry introspection settings, you must be familiar with the Introspection module. For details, see "Understanding the vGW Series Introspection Module" on page 85 and in particular the other topics identified in the Related Topics section of this topic.

Copyright © 2015, Juniper Networks, Inc.

This example assumes that you want vGW Series to scan for data in key HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec AntiVirus\Install\7.50.

1. On the Introspection > Settings > vGW Application Settings > Registry Values page, configure a new registry key. See Figure 54 on page 107.

Figure 54: Configuring a New Registry Key



a. In the **Name:** field, enter **Install Directory of AV**.

b. In the Key: field, enter **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec AntiVirus\Install\7.50**.

> WARNING: The Key that you enter must begin with the prefix HKEY_LOCAL_MACHINE\. This is the only registry root that vGW Security VM currently supports. If the key that you enter does not contain this prefix, vGW Series displays the following alert message and highlights the Key input field.
>
> Currently only registry values under root HKEY_LOCAL_MACHINE are supported. Please enter a key that starts with HKEY_LOCAL_MACHINE.

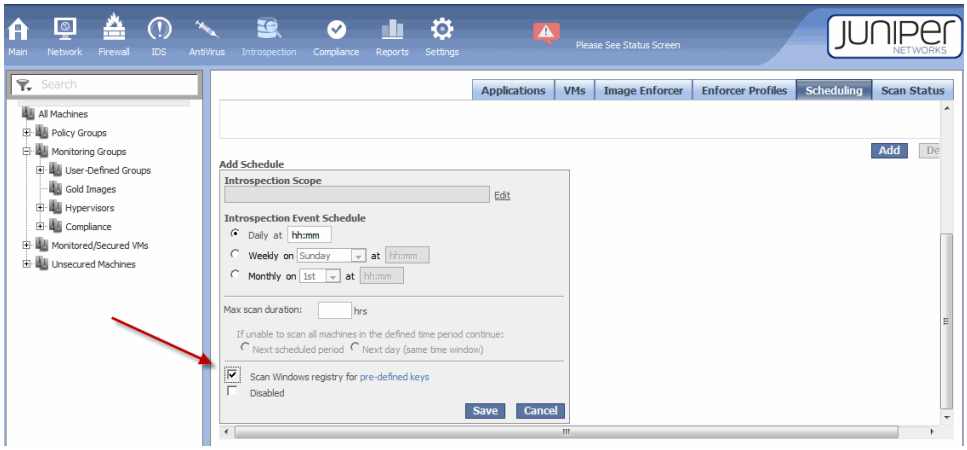
c. In the **Value Name:** field, enter **InstallDir**.

d. In the Data: field, enter **C:\Program Files\Symantec\Symantec Endpoint Protection**. This is the enforcer data.

2. To include this and all other configured Registry Values in a scheduled scan:

   a. Check the option **Scan Windows registry for pre-defined keys** on the Introspection module Scheduling tab > Add Schedule pane. See Figure 55 on page 108.

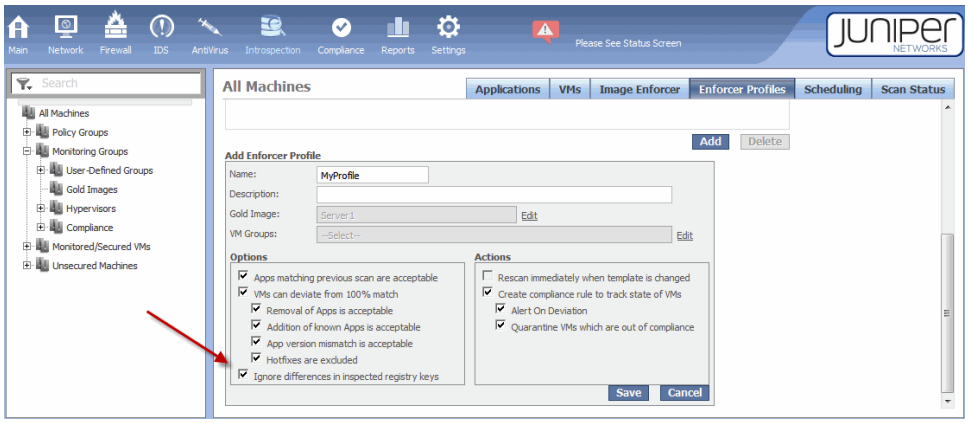
Figure 55: Add Schedule for Scan Page



To include this and all other configured Registry Values in an Enforcer Profile.

1. On the **Introspection** > **Enforcer Profile** > **Add Enforcer Profile** pane, create a profile.
2. Ensure that the **Ignore differences in inspected registry keys** check box is not selected. See Figure 56 on page 108.

Figure 56: Add an Enforcer Profile that Allows for Registry Scans



   Now scans that you initiate by clicking **Scan Now** on the Introspection > Scan Status page will scan registry keys.

To use registry values in a Smart Group:

1. On the Settings > Security Settings > Groups page, add your Smart Group.
2. Use the **vf.app.registry** smart property with the **contains** operator to add your condition. The value of **vf.app.registry** property will be all registry keys and their data concatenated, for example: **[key1\val1=data1,key2\val2=data2]**.

Copyright © 2015, Juniper Networks, Inc.

Use the Introspection module > Applications tab or the Introspection module > VMs tab to view the results of scans. The registry values will appear in the **Name** column, with their data in the **Version** column.

Related Documentation

- Understanding the vGW Series Introspection Registry Check Feature on page 105
- Understanding the vGW Series Introspection Scheduling Feature on page 101
- Understanding the vGW Series Introspection Scan Status on page 102
- Understanding the vGW Series Introspection Image Enforcer Feature on page 93
- Understanding the vGW Series Introspection Applications Tab on page 87
- *Understanding vGW Series*
- Understanding the vGW Series Introspection Module on page 85

Copyright © 2015, Juniper Networks, Inc.

PART 4

Quarantine

- Quarantined VMs on page 113

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 12

Quarantined VMs

- Understanding Quarantined VMs and How to Manage Them on page 113

Understanding Quarantined VMs and How to Manage Them

This topic covers aspects of the vGW Series quarantine feature. When a VM is quarantined as a result of a vGW AntiVirus, Compliance, or Image Enforcer scan, the VM is added to the Quarantine Policy group in the VM tree.

When a VM is added to the Quarantine Policy group, the quarantine policy that you configured using the Firewall module is applied to it. After a VM is quarantined, at any time, you can use the Main module Quarantine tab to manage it in various ways.

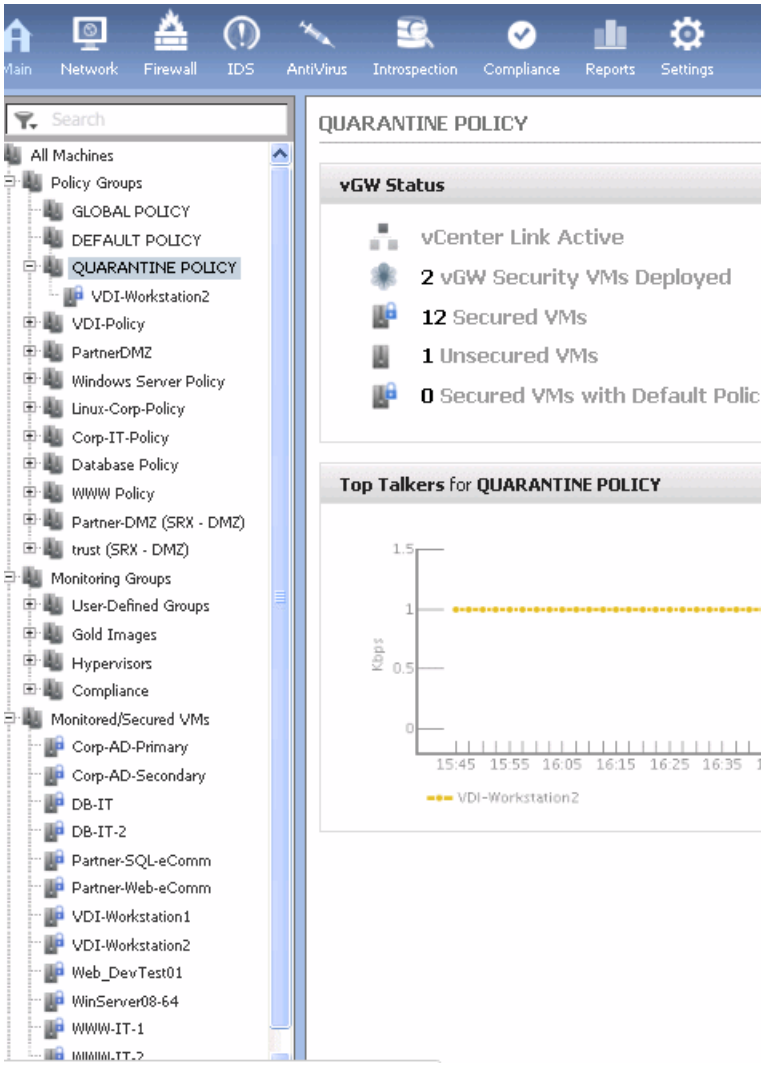
The Quarantine Policy group, the quarantine policy associated with it, and the Main module Quarantine tab cooperate to help you control and manage quarantined VMs. This topic includes the following sections:

- About vGW Series Quarantine on page 113
- Configuring a Quarantine Policy on page 114
- Viewing the Quarantined VMs, Releasing Them From Quarantine, and Resolving Problems on page 115

About vGW Series Quarantine

The Quarantine Policy group belongs to the Policy Groups branch. Figure 39 on page 66 shows that one quarantined VM has been added to the Quarantine Policy group.

Figure 57: Quarantine Policy in the VM Tree

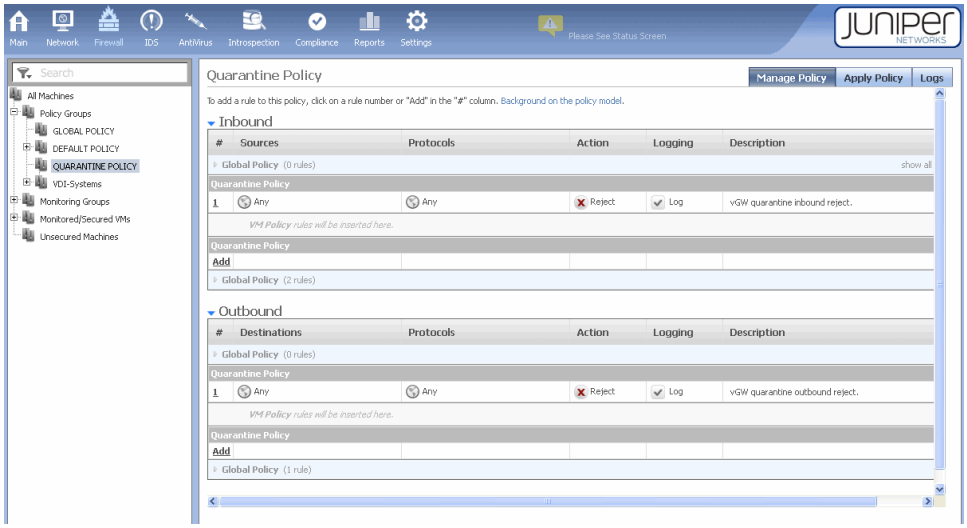


Configuring a Quarantine Policy

The Firewall module allows you to configure policy rules, including configuring a quarantine policy. You use the Quarantine Policy page for this purpose.

Copyright © 2015, Juniper Networks, Inc.

Figure 58: Configuring a vGW Series Quarantine Policy



To display the Quarantine Policy page:

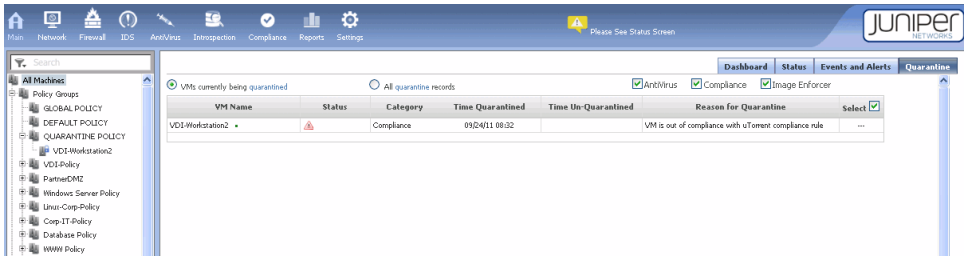
1. Select the Firewall module on the taskbar.
2. Select the Quarantine Policy group.
3. Configure the policy rules. For details on configuring policy rules, see "Understanding the vGW Series Firewall Module" on page 11.

Viewing the Quarantined VMs, Releasing Them From Quarantine, and Resolving Problems

The Main module Quarantine tab page displays a table that includes a row for each quarantined VM. You can display information for VMs quarantined as a result of vGW AntiVirus, Compliance, and Image Enforcer scans. You can display information for all quarantined VMs or VMs by scan category.

The table identifies the time the VM was quarantined and the reason for it. See Figure 41 on page 67.

Figure 59: Main Module Quarantine Tab



To view a quarantined VM in the quarantine table, resolve the problem, and remove it from quarantine:

1. Select the Main module in the taskbar.
2. Select the Quarantine tab.
3. To remove the VM from quarantine, select the VM and click **Un-Quarantine VM**.
4. Resolve the problem that caused the VM to be quarantined.

   Removing a VM from quarantine does not fix the underlying problem that caused the VM to be quarantined. A VM might be quarantined because of a compliance, image enforcer, or vGW AntiVirus violation.

   You can fetch the VM to resolve it offline or you can delete the VM.

Related Documentation

- *Understanding vGW Series*
- Understanding vGW Series AntiVirus on page 51
- Configuring vGW Series AntiVirus On-Access Scanning on page 75
- Configuring vGW Series AntiVirus On-Demand Scanning on page 78
- Understanding the vGW Series Enforcer Profiles Tab on page 95

Copyright © 2015, Juniper Networks, Inc.

PART 5

Compliance

- Compliance Module and Hypervisor on page 119

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 13

Compliance Module and Hypervisor

- Understanding the vGW Series Compliance Module on page 119
- Configuring a Compliance Rule on page 121
- Understanding the vGW Series Hypervisor and Extended VM Security on page 124

Understanding the vGW Series Compliance Module

This topic covers the Compliance module of the vGW Security Design VM that lets you monitor the compliance of your overall system with regard to industry standards best practices. Additionally, you can define rules that reflect your organization's best practices. That is, rather than using only industry best practices or standards guidelines such as PCI and HIPAA, you can define your own compliance requirements.

This topic contains the following sections:

- The Compliance Module on page 119
- The Compliance Tab on page 120
- The Rules Tab on page 121

The Compliance Module

The Compliance module relies on a rule editor that allows you to use multiple attributes about the VMware infrastructure and associated VMs to establish criteria for each designed rule. The Compliance module supports both IPv4 and IPv6 addresses. You can use any of the vGW Series built-in compliance rules in both IPv4 and IPv6 environments.

By using compliance rules to monitor key configuration parameters, you can quickly ascertain the overall state of your virtual security system. For example, you can create a compliance rule that states that non-administrative VMs are not allowed to be connected to a specific port group.

Violation of the designated rules impacts the overall compliance state. You can view details on the violations in the reports and status pages.

Copyright © 2015, Juniper Networks, Inc.

NOTE: If you are not using the Compliance module, you can disable it to lessen the amount of time that it takes to log into the vGW Security Design VM and improve runtime performance.

To disable the Compliance module, in center.conf set the following property to false:

center.enable.compliance.onrestart

After you change the property value, you must restart the system.

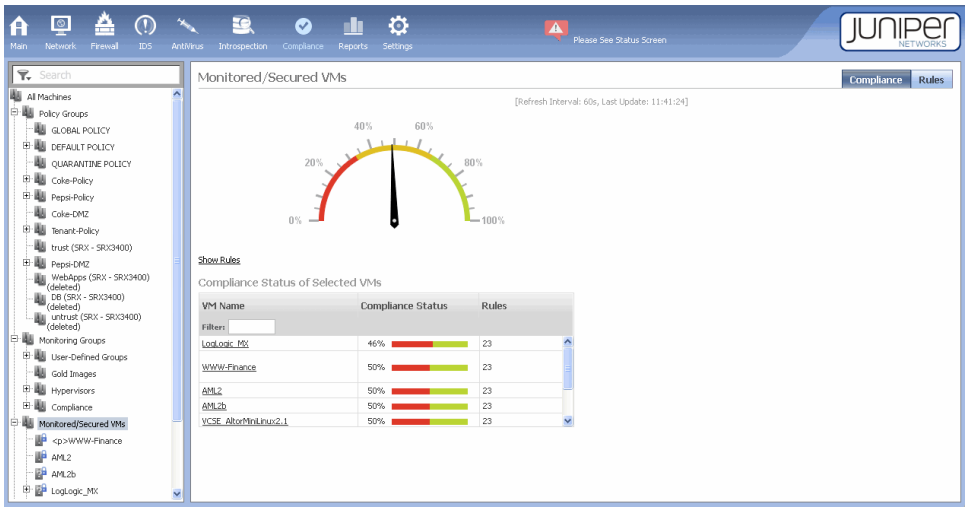
The Compliance page contains two tabs:

- Compliance
- Rules

The Compliance Tab

The Compliance tab displays a compliance meter that indicates the current level of compliance for the VM or group of VMs selected in the VM tree. It also shows statistical data that was used to calculate the overall compliance level.

Figure 60: vGW Series Compliance Module



To reflect the current compliance level, the compliance meter is refreshed automatically at 60 second intervals.

If you selected a VM group in the VM tree, the compliance meter shows the overall compliance percentage for all VMs in the group. The table below the meter lists each VM by name and shows its individual compliance level.

To display the compliance rules associated with the group, click **Show Rules**. A table appears listing each rule. It gives the name, weight, the number of VMs that the rule applies to, and the compliance status of the rule.

Copyright © 2015, Juniper Networks, Inc.

- To disable a rule, clear its check box.

  The compliance meter is refreshed, indicating the current level of compliance with the adjusted rule set.

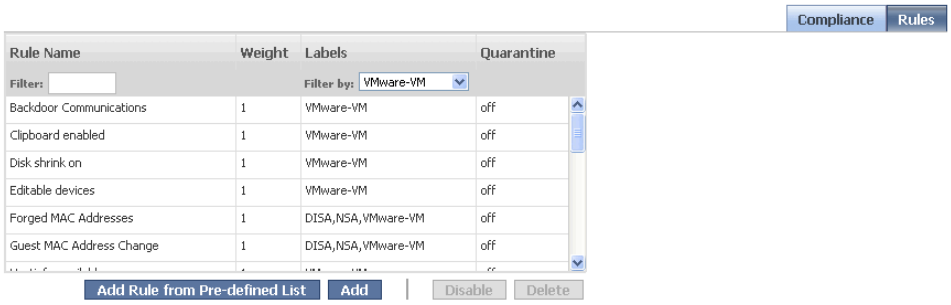
- Double-click a rule in the table to display details about the rule.

If you selected a single VM in the VM Tree, the compliance meter displays the current compliance of the individual machine and the rules protecting it.

The Rules Tab

The Rules tab allows you to create and manage compliance rules. This tab includes a list of defined rules that includes the name of the rule, its weight, and any labels associated with it. Labels group rules in categories.

Figure 61: vGW Series Compliance Module Rules Tab



You can narrow the list of rules displayed using the **Filter by** menu.

NOTE: vGW Series provides several built-in compliance rules and templates which assess the virtual infrastructure against security and hardening guidelines from VMware. These rules are also good examples to use to learn how the Compliance module works. You can use these built-in compliance rules in both IPv4 and IPv6 environments.

Related Documentation

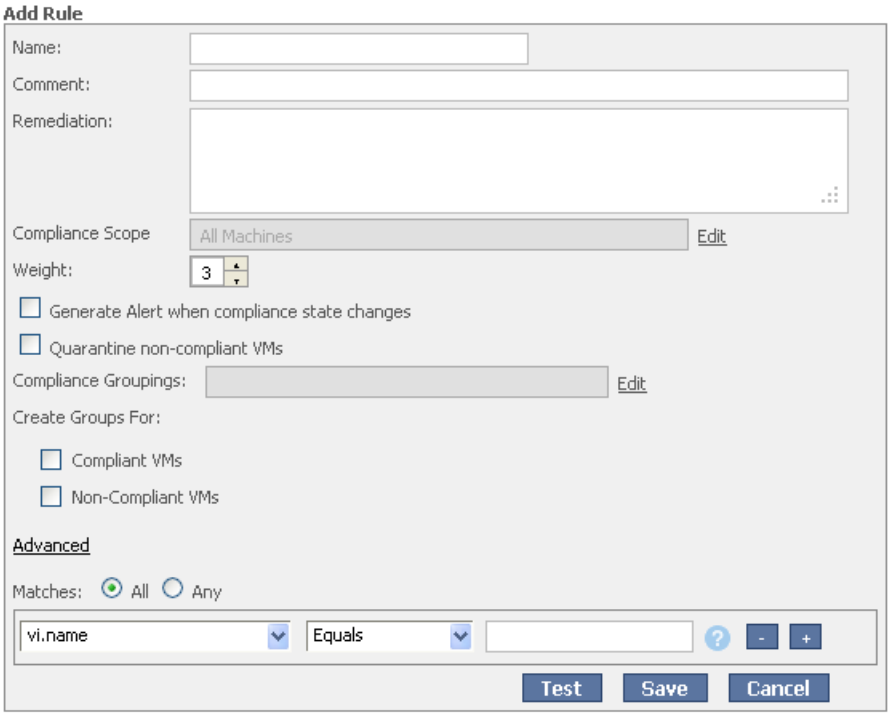
- *Understanding vGW Series*

Configuring a Compliance Rule

This topic explains how to create a compliance rule. For an overview of the Compliance module, see "Understanding the vGW Series Compliance Module" on page 119.

To create a compliance rule:

1. From the Compliance module > Rules tab, click Add. The Add Rule dialog box appears.



2. Define the rule. Table 12 on page 122 describes the available options.

Table 12: Compliance Rule Creation Parameters

Option	Action
Compliance Scope	Select **All Machines** or **Selected Group**, and then choose a group from the list.
Name	Enter a name for the rule. Rule names can contain characters and numbers and should be descriptive, yet simple. You can describe the rule in more detail in the **Comment** field, if needed.
Weight	Enter a weight to be used when calculating the compliance level.
Generate Alert when compliance state changes	Direct the vGW Series to post a warning when the compliance level changes.
Compliance Groupings	Click **Edit**, move one or more labels to the **Selected Labels** list, and then click **Apply**.
Create Groups	Create groups comprised of members who meet or violate the designated match criteria (defined in the **Matches** field). You are not required to create groups, but if you do select one of the two options, you will by default create a non-policy, Smart Group. This group can be changed to a Policy group through Settings -> Security Settings -> Groups. The benefit of automatically creating a compliance-based group is that you can easily find VMs in the VM Tree using this criterion and use the group throughout the vGW Series Table 12 on page 122.

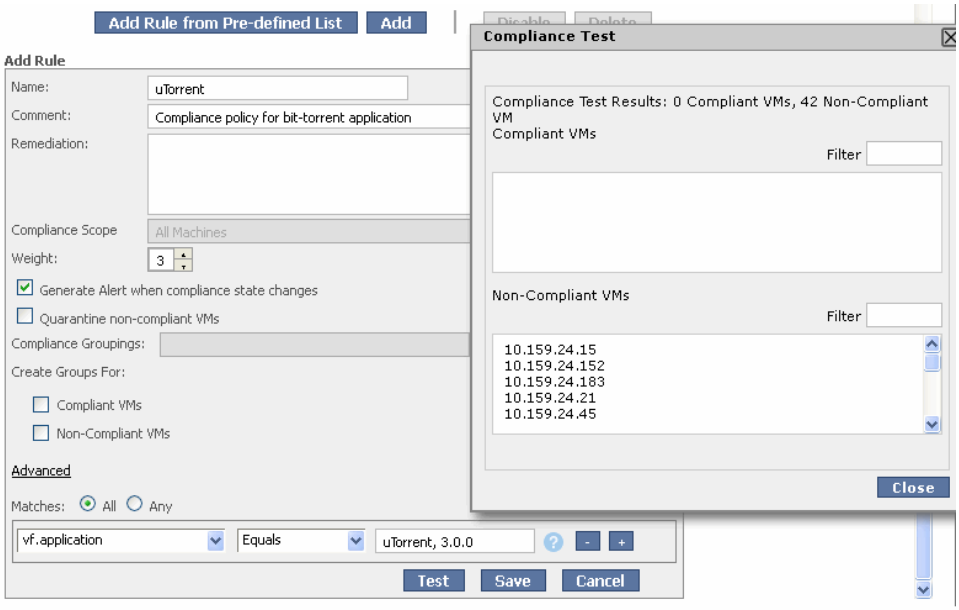
Copyright © 2015, Juniper Networks, Inc.

Table 12: Compliance Rule Creation Parameters *(continued)*

Option	Action
Matches	Select **All** if the VM must meet all criteria defined in field below or **Any** if the VM can meet any of the criteria defined in the field below, and then choose an attribute, choose an operator, and enter a value. • To add another criterion to the rule, click **+**. • Click **-** to remove a criterion from the rule.
Advanced	Enter a selection query rather than defining. For information about query syntax.

3. Click **Test**.

   The vGW checks your criteria and posts a message in the Edit Rule dialog box indicating which VMs are included in the group (if any), given the criteria you specified.



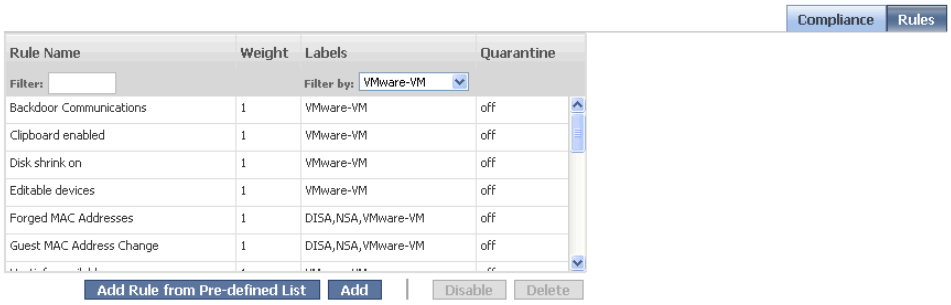
4. Click **Save**.

NOTE: In addition to the items described in Table 12 on page 122, you also have the option of disconnecting VMs from the network during a compliance check. By default this option is hidden because if it is used incorrectly it can cause serious problems resulting in unintended network downtime. For example, if you created a compliance rule with this action incorrectly, you could bring all VMs offline. To enable this compliance action, execute the following command from within the Web interface of the vGW Security Design VM. After it is executed, you will see a selection box called “Disconnect from the network when non compliant”.

http:///compDisconnect?disconnect=true (or false)

You can select a predefined rule to use. To facilitate your search for a rule, you can specify a filter.

Figure 62: Adding a Predefined Compliance Rule



If DHCP is available, you can determine the IP address from the vCenter server. To do so, select the **vGW Security Design VM** in the vCenter console, and then select the **Summary** tab. Alternatively, you can display the IP address by selecting the **Console** tab.

By default, the vGW Security Design VM is configured for dual stack, with IPv4 configured to use DHCP and IPv6 configured to use stateless autoconfiguration.

NOTE: By default, a dual stack vGW Security Design VM communicates with a vGW Security VM using the IPv4 protocol. However, you can use the vGW CLI to change the default IP protocol used by setting the center.dual.stack.default.communication.ipv4 parameter to false.

center.dual.stack.default.communication.ipv4=false

By default, this parameter is set to **true**.

This parameter is relevant only if the vGW Security Design VM is configured for dual stack and one or more vGW Security VMs is also configured for dual stack. In all other cases, the protocol used is the one that is common to both the vGW Security Design VM and the vGW Security VM, and this parameter is irrelevant.

Related Documentation

- *Understanding vGW Series*

Understanding the vGW Series Hypervisor and Extended VM Security

This topic covers vGW Series security for the hypervisor and VMs that aligns with VMware hardening guidelines. Before you read this topic, read *Understanding Hypervisors and vGW Series*.

Copyright © 2015, Juniper Networks, Inc.

NOTE: To benefit from this content, you should have a general understanding of VMware hardening guidelines.

- The Need for Hypervisor Security on page 125
- vGW Series Hypervisor and VM Security, and VMware Hardening Guidelines on page 125
- vGW Series Hypervisor and VM Security Overview on page 125
- Remediation on page 126
- Configuration Example on page 126

The Need for Hypervisor Security

In full virtualization, a layer, commonly called the hypervisor or the virtual machine monitor, exists between the virtualized operating systems and the hardware. This layer multiplexes the system resources between competing operating system instances.

In the hypervisor, the virtualization infrastructure introduces a new layer of abstraction with potential exposure for malware attacks. Attempts to exploit the hypervisor as a target for attacks have increased in the recent past, and they are expected to continue to increase in number and kind in the near future. Attacks on the hypervisor can cause serious disruption such as compromise of sensitive data and denial of service (DoS). Any exposure on the hypervisor can expose guest virtual machines (VMs) that belong to many different tenants. Because the hypervisor is a crucial resource in the virtualized environment, protection of it is vital to overall security.

vGW Series enables you to verify that the hypervisor hosts that you secure meet security and compliance standards needed for a secure environment. The built-in hypervisor compliance checks are based on VMware security hardening guidelines. Additional custom hypervisor compliance checks can be created to automate any needed security compliance checks. You can use the built-in hypervisor compliance checks for hypervisors that have either an IPv4 or IPv6 address.

vGW Series Hypervisor and VM Security, and VMware Hardening Guidelines

vGW Series hypervisor security aligns with VMware hardening guidelines in all ways that are possible. vGW Series does not implement all guidelines for certain reasons. For example:

- Some guidelines, such as “NCN12 - document VLANs used on vSwitches”, pertain to behavior that can be implemented in various ways. Because of the varied implementation, the vGW Series cannot check for violations.
- Some guidelines, such as “HST02 - Ensure uniqueness of CHAP auth secret”, pertain to components inaccessible to the vGW Series. Therefore, vGW cannot perform checks on them.

vGW Series Hypervisor and VM Security Overview

You use the Security Design VM to view and configure information for the hypervisor. You can quickly view the vGW Series compliance checks that correspond with VMware

recommendations by selecting **VMware-VM** and **VMware-host** in the filter box displayed on the Compliance module Rules tab.

When you select a rule, a pane is displayed that explains the rule and the remediation action to take in response to compliance violations.

From the **Edit Rule** pane, you can modify the definition of the rule in the following ways. You can change:

- The scope of groups that the rule applies to, in the Compliance Scope list.

  Click **Edit** to display the list of configured VMs and groups.
- The rule weight, in the **Weight** field, from 1–5.
- Whether an alert is generated when the compliance state of a hypervisor or a VM that belongs to the group changes.
- Whether non-compliant VMs and hypervisors should be quarantined.
- Whether the vGW Security Design VM should automatically create hypervisors groups for **Compliant VMs** and **Non-Compliant VMs**.

Remediation

For each compliance check (rule), specific remediation is suggested. You can also refer to the VMware hardening guidelines for additional information.

Configuration Example

To configure compliance requirements for hypervisors and view information about them, you the VM Tree in conjunction with the Compliance module.

1. Under Monitoring Groups in the VM Tree, select the Hypervisors group to display the Hypervisor page.

   The Hypervisors page shows the following information:

   - The overall compliance status for the ESX/ESXi hosts in your virtualized environment.
   - For individual hypervisors that belong to the Hypervisors monitoring group, the Compliance Status of Selected VMs table shows the hypervisor IP address, its compliance status, and the number of compliance rules configured for it.
2. To display information about the rules configured for the hypervisors in the group, click **Show Rules**.

   The Hypervisors page expands to show the following information:

   - The **Compliance Rules for Selected VMs** table. This table shows the complete set of rules configured for the hypervisors. For each rule, it shows the following information:
     - The rule name.
     - The weight that is given to the rule.
     - The VMs—in this case, hypervisors—that the rule applies to.

 Copyright © 2015, Juniper Networks, Inc.

  - The **Quarantine** state, that is, whether quarantine is enabled for the rule.
  - The overall compliance status of the hypervisors that the rule is assigned to.
- The **Compliance Status of Selected VMs** table that shows the following information:
  - The IP address of the hypervisor.
  - The compliance status of the hypervisor in regard to all the rules that are applied to it.
  - The number of rules that apply to it.

3. To display the configuration of any rule, in the Compliance Rules for Selected VMs table, click the rule name.

   The **Edit Rule** pane is displayed. It shows the following information:

   - Beneath the name of the rule, a **Comment** field giving a brief description of it.
   - A **Remediation** field that suggests a remediation action that you can take to bring the hypervisor into conformance with the rule.

   From the **Edit Rule** pane, you can modify the definition of the rule in the following ways. You can change:

   - The scope of groups that the rule applies to, in the Compliance Scope list. Click **Edit** to display the list.
   - The rule weight, in the **Weight** field, from 1–5.
   - Whether an alert is generated when the compliance state of a hypervisor that belongs to the group changes.
   - Whether non-compliant hypervisors should be quarantined.
   - Whether the vGW Security Design VM should automatically create hypervisors groups for **Compliant VMs** and **Non-Compliant VMs**.
4. To customize the rule's syntax, from the **Edit Rule** pane for the rule, click **Advanced**. For details on configuring Smart Group definitions, see *Understanding vGW Series Smart Groups*.
5. Click **Test** to test the rule against hypervisors in the selected scope, after you configure the rule.
6. After you are satisfied with the rule definition, click **Save**.

Related Documentation

- *Understanding vGW Series*

Copyright © 2015, Juniper Networks, Inc.

PART 6

Index

- Index on page 131

Copyright © 2015, Juniper Networks, Inc.

Index

Symbols

#, comments in configuration statements....xv
( ), in syntax descriptions....xv
< >, in syntax descriptions....xv
[ ], in configuration statements....xv
{ }, in configuration statements....xv
| (pipe), in syntax descriptions....xv

A

AntiVirus....51
    overview....51

B

braces, in configuration statements....xv
brackets
    angle, in syntax descriptions....xv
    square, in configuration statements....xv

C

comments, in configuration statements....xv
Compliance module....119
conventions
    text and syntax....xiv
curly braces, in configuration statements....xv
customer support....xvi
    contacting JTAC....xvi

D

documentation
    comments on....xv

E

Enforcer Profiles tab....95

F

Firewall module....11
    used with Network module....8
firewall policy rules for vGW components....38
font conventions....xiv

G

Gold Image....94, 95

I

ICMPv6P....24
Image Enforcer
    Enforcer Profiles tab....95
    Gold Image....94
    Image Enforcer tab....94
Introspection module
    Applications feature....87
    Image Enforcer....94, 95
    Scan Status feature....102
    Scheduling feature....101
    VMs tab....90

M

manuals
    comments on....xv

N

Network module....3
    used with Firewall module....8

P

parentheses, in syntax descriptions....xv
Primary-level entry
    secondary-level entry....28
Primary-level entry only....28
Protocols
    ICPMv6....24

S

support, technical *See* technical support
syntax conventions....xiv

T

technical support
    contacting JTAC....xvi

V

vGW AntiVirus
    On-Access scanning....75
vGW Security Design VM
    Firewall module....8, 11
    Introspection module....101, 102
        Applications feature....87
        VMs tab....90

Network module.....3, 8
predefined firewall policy rules 38
vGW Security Design VM modules
Compliance module.....119
vGW Security VM
predefined firewall policy rules 38

Copyright © 2015, Juniper Networks, Inc.