

Firefly Host

Getting Started Guide for VMware

Release

6.0



Published: 2014-06-23

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2014, 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.

Firefly Host Getting Started Guide for VMware
Release 6.0
Copyright © 2014, 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.

Abbreviated Table of Contents

	About The Documentation	xv
Part 1	Firefly Host Overview	
Chapter 1	Introduction to Firefly Host	3
Chapter 2	Firefly Host Dashboard and Firefly Host VM	11
Chapter 3	Firefly Host Dashboard Navigation and VM Tree	27
Chapter 4	Status and Alerts	35
Part 2	VMware and Firefly Host	
Chapter 5	Overview	39
Chapter 6	OVA and Firefly Host Deployment	47
Part 3	Firefly Host Setup	
Chapter 7	Firefly Host Dashboard Setup Process	61
Part 4	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 8	Securing ESX/ESXi Hosts using Firefly Host	75
Chapter 9	Firefly Host Firewall Module	79
Chapter 10	Firefly Host Network Module	109
Part 5	Index	
	Index	119

Table of Contents

	About The Documentation	xv
	Documentation and Release Notes	xv
	Documentation Conventions	xv
	Documentation Feedback	xvii
	Requesting Technical Support	xviii
	Self-Help Online Tools and Resources	xviii
	Opening a Case with JTAC	xviii
Part 1	Firefly Host Overview	
Chapter 1	Introduction to Firefly Host	3
	Understanding Firefly Host	3
	Understanding the Firefly Host Architecture	4
	Understanding Cloud Computing and Firefly Host	6
	Understanding the VMware Infrastructure and Firefly Host	7
	Understanding vSphere and the Firefly Host	7
	Understanding VMware ESX and ESXi Hosts and the Firefly Host	7
	Understanding VMotion and Firefly Host	8
	Understanding Hypervisors and Firefly Host	9
Chapter 2	Firefly Host Dashboard and Firefly Host VM	11
	Understanding the Firefly Host Dashboard	11
	Firefly Host Dashboard Modules (VMware)	12
	Understanding the Firefly Host Main Module	17
	Dashboard	17
	Status Tab	18
	Events and Alerts Tab	20
	Security Alerts	21
	System Status and Events	22
	Quarantine Tab	23
	Understanding the Firefly Host VM	24
	Understanding the Firefly Host Module	24
Chapter 3	Firefly Host Dashboard Navigation and VM Tree	27
	Understanding Firefly Host Dashboard Navigation	27
	Understanding the Firefly Host Dashboard Taskbar	29
	About the Firefly Host Dashboard Tree	30
	VM Tree Overview	31
	Locating VMs in a Complex VM Tree	32

Chapter 4	Status and Alerts	35
	Understanding Firefly Host Status and Alerts	35
	Status	35
	Alerts	35
Part 2	VMware and Firefly Host	
Chapter 5	Overview	39
	Firefly Host Prerequisites and Resource Requirements for the VMware	
	Environment	39
	Overall Resource and Access Requirements	39
	Virtual Appliance System Requirements	40
	Firefly Host VMware vSwitch Requirements	41
	VMware Port Group Requirements	42
	Virtualized NIC Requirements	43
	Preparing to Integrate Firefly Host with the VMware Environment	43
	Understanding Firefly Host Environment Time Synchronization	44
	Firefly Host VMsafe Firewall + Monitoring and VMsafe Monitoring Modes	44
Chapter 6	OVA and Firefly Host Deployment	47
	Understanding the Open Virtualization Format OVA Template Method	47
	Using the OVA Bundled Method to Integrate Firefly Host with the VMware	
	Infrastructure	48
	Using the OVA Single File Method to Integrate the Firefly Host Dashboard with	
	VMware	56
	Using the OVA Single File Method to Integrate the Firefly Host VM with	
	VMware	58
Part 3	Firefly Host Setup	
Chapter 7	Firefly Host Dashboard Setup Process	61
	Setting Up Firefly Host	61
	Determining the Firefly Host Dashboard's Default IP Address	61
	Changing or Setting the IP Address for the Firefly Host Dashboard	63
	Connecting to the Firefly Host Dashboard and Configuring Basic	
	Settings	64
Part 4	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 8	Securing ESX/ESXi Hosts using Firefly Host	75
	Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard	75
	Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is	
	Unsecured	76
	Displaying the State of the vmsafe config Setting	76
	Disabling the Suspend-Resume Process	76
	Understanding Automatic Securing of VMs	77

Chapter 9	Firefly Host Firewall Module	79
	Understanding the Firefly Host Firewall Module	79
	The Firewall Module and the VM Tree	79
	Overview of the Firewall Policy Model	80
	Global Policy, Group Policy, and Individual VM Policy Tiers	81
	Global Policy	82
	Group Policy	83
	Individual VM Policy Rules	84
	Default Policy	84
	Quarantine Policy	84
	Firewall Policy Structure and Policy Rules Precedence	84
	Viewing the Complete Policy Rule Base for a VM	86
	The Manage Policy Tab	86
	Policy Per vNIC and Dual Stack	87
	Creating a Policy Rule	87
	The Apply Policy Tab	90
	The Logs Tab	92
	Understanding How Firefly Host Handles ICMPv6 Protocol Traffic	93
	About ICMPv6	93
	Filtering ICMPv6 Packets	93
	Default Policy Group for Allowing Inbound ICMPv6 Packets	94
	Viewing the Default ICMPv6 Protocols Group Members	94
	Editing the Default ICMPv6 Protocols Group Members	96
	Understanding Predefined Objects for Firefly Host Firewall Policy Terms	97
	Defining and Selecting Source and Destination Terms for Policy Rules	97
	Predefined Global IP Address Objects	97
	Predefined Network Objects	98
	Predefined Network Objects for Well Known IP Addresses	98
	Additional IPv4 and IPv6 Predefined Network Objects	99
	Configuring Firefly Host Firewall Policies	100
	Understanding Firefly Host Predefined Firewall Policy for Its Components	107
Chapter 10	Firefly Host Network Module	109
	Understanding the Firefly Host Network Module	109
	Network Module	109
	Manipulating Displayed Information	110
	Changing the Time Interval for Displayed Information	111
	Using Advanced Options for Filtering Network Data	113
	Sorting Table Data	113
	Using the Firefly Host Network and Firewall Modules Cooperatively	114
	Network Assessment	114
	Using the Network Module to Observe Traffic Coming Into and Going Out from VMs	115
	Detecting Unexpected and Unwanted Behavior	115
	Using the Network and Firewall Modules Together	116
Part 5	Index	
	Index	119

List of Figures

Part 1	Firefly Host Overview	
Chapter 1	Introduction to Firefly Host	3
	Figure 1: Firefly Host Architecture	5
	Figure 2: Pop-Up Box Displayed During Firefly Host VM install/un-install Process	8
	Figure 3: Problem Resolution Message for vMotion Halt	9
Chapter 2	Firefly Host Dashboard and Firefly Host VM	11
	Figure 4: Main Module Displayed at Login	12
	Figure 5: Main Module	13
	Figure 6: Network Module	13
	Figure 7: Firewall Module	14
	Figure 8: IDS Module	14
	Figure 9: AntiVirus Module	15
	Figure 10: Introspection Module	15
	Figure 11: Compliance Module	16
	Figure 12: Reports Module	16
	Figure 13: Settings Module	17
	Figure 14: Dashboard Tab	18
	Figure 15: Status Tab	19
	Figure 16: Taskbar Showing the Health Status Icon	20
	Figure 17: Main Module Events and Alerts Page	21
	Figure 18: Consolidated Logs for Events and Alerts	21
	Figure 19: Quarantine Tab	23
Chapter 3	Firefly Host Dashboard Navigation and VM Tree	27
	Figure 20: Firefly Host Dashboard Taskbar	27
	Figure 21: VM Tree	28
	Figure 22: Firefly Host Dashboard Taskbar	29
	Figure 23: VM Tree with Selected VMs	31
	Figure 24: Searching All VMs in the VM Tree Using the Advanced Editor	33
	Figure 25: Searching for Specific VMs in the VM Tree Using the Advanced Editor	34
Part 2	VMware and Firefly Host	
Chapter 6	OVA and Firefly Host Deployment	47
	Figure 26: OVA Template Details Page	50
	Figure 27: OVA File Deployment License Agreement	50
	Figure 28: Naming the vApp	51
	Figure 29: Specifying the Host and Cluster	52

	Figure 30: Selecting the Storage	52
	Figure 31: Mapping the Firefly Host Management Networks	53
	Figure 32: Specifying the Database Disk Size	54
	Figure 33: Verifying That the Configuration Is Correct	54
	Figure 34: Displaying the Firefly Host Appliance Components	55
	Figure 35: Firefly Host Dashboard Summary Tab in vCenter	56
Part 3	Firefly Host Setup	
Chapter 7	Firefly Host Dashboard Setup Process	61
	Figure 36: Viewing the Firefly Host Dashboard IP Address in VMware	62
	Figure 37: Firefly Host Dashboard IP Addresses on the Firefly Host CLI Console	63
	Figure 38: Configuring an IP Address for the Firefly Host Dashboard	63
	Figure 39: Logging In to the Firefly Host Dashboard	64
	Figure 40: Firefly Host Installation Wizard Overview	65
	Figure 41: Changing the Default Password	65
	Figure 42: Configuring Network Settings for the Firefly Host Dashboard	67
	Figure 43: Configuring the Time Server	68
	Figure 44: Firefly Host Installation Wizard displaying Product Licensing	69
	Figure 45: Firefly Host Dashboard vCenter Integration	70
	Figure 46: Configuring the Firefly Host Dashboard vCenter Settings	71
Part 4	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 9	Firefly Host Firewall Module	79
	Figure 47: Firewall Module Policy for a Single VM	80
	Figure 48: Global Policy	83
	Figure 49: VM Policy Expanded Rule Base	86
	Figure 50: Firewall Module Manage Policy Page	87
	Figure 51: Adding a Rule	88
	Figure 52: Using the Dialog Box Filter to Add Terms for policy rules	88
	Figure 53: Firewall Apply Policy Page	90
	Figure 54: Changed Policies Dialog Box	91
	Figure 55: Firewall Module Logs Tab	92
	Figure 56: Default Global Policy Showing Default ICMPv6 Allow Group	94
	Figure 57: Protocols Settings ICMPv6 Default Protocol Group	95
	Figure 58: Default Global Policy	102
	Figure 59: Adding a Global Policy Rule to Reject Telnet Connection Attempts	103
	Figure 60: VM Policy for an Individual VM	105
	Figure 61: Complete VM Policy for an Individual VM	105
	Figure 62: All Machines	106
	Figure 63: Policy Install Progress	106
Chapter 10	Firefly Host Network Module	109
	Figure 64: Network Summary Tab for All VMs	110
	Figure 65: Main Module Network Module Summary Tab for a Single VM	110
	Figure 66: Displaying Network Data for Different Time Intervals: Part 1	111
	Figure 67: Displaying Network Data for Different Time Intervals: Part 2	111
	Figure 68: Selecting a Time Interval	112

Figure 69: Setting the Custom Time Period	112
Figure 70: Top Protocols Across All Machines Example	114
Figure 71: Network Module Connection Tab Information	115

List of Tables

	About The Documentation	xv
	Table 1: Notice Icons	xvi
	Table 2: Text and Syntax Conventions	xvi
Part 1	Firefly Host Overview	
Chapter 2	Firefly Host Dashboard and Firefly Host VM	11
	Table 3: Firefly Host Status Icons	19
Chapter 3	Firefly Host Dashboard Navigation and VM Tree	27
	Table 4: Taskbar Icons	29
	Table 5: Virtual Machine State Icons	32
Part 2	VMware and Firefly Host	
Chapter 5	Overview	39
	Table 6: Firefly Host Dashboard Specifications	41
	Table 7: Firefly Host VM Specifications	41
Part 4	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 9	Firefly Host Firewall Module	79
	Table 8: Firewall Policy Configuration Settings	89
	Table 9: Firewall Policy Icons	91
Chapter 10	Firefly Host Network Module	109
	Table 10: Using Advanced Options for Filtering Network Data	113

About The Documentation

- Documentation and Release Notes on page xv
- Documentation Conventions on page xv
- Documentation Feedback on page xvii
- Requesting Technical Support on page xviii

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 xvi 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 xvi 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
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	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 <i>domain-name</i>

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.	<ul style="list-style-type: none">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 <i>metric</i>>;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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 [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(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.	<ul style="list-style-type: none">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).

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

PART 1

Firefly Host Overview

- [Introduction to Firefly Host on page 3](#)
- [Firefly Host Dashboard and Firefly Host VM on page 11](#)
- [Firefly Host Dashboard Navigation and VM Tree on page 27](#)
- [Status and Alerts on page 35](#)

CHAPTER 1

Introduction to Firefly Host

- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host Architecture on page 4](#)
- [Understanding Cloud Computing and Firefly Host on page 6](#)
- [Understanding the VMware Infrastructure and Firefly Host on page 7](#)
- [Understanding Hypervisors and Firefly Host on page 9](#)

Understanding Firefly Host

Firefly Host delivers complete virtualization security for multitenant public and private clouds, and clouds that are a hybrid of the two. Firefly Host is built off the vGW product line and replaces it. Firefly Host comprises the following three main components:

- The Firefly Host Dashboard that provides a central management server. It consists of a set of modules that you use to configure the Firefly Host features for your virtualized environment. It provides charts, tables, and graphs that allow you to view information that Firefly Host produces about your environment and use in determining how to adjust your security policy.

You use it to install and manage the Firefly Host VMs that you deploy to secure hosts in your virtualized environment.

- The Firefly Host VM that is installed on each host to be secured. The Firefly Host VM acts as a conduit to the Firefly Host Module that it inserts into the hypervisor of the host that Firefly Host protects. The Firefly Host VM maintains policy and logging information. A Firefly Host VM remains attached to the ESX/ESXi host that it is installed on.

The Firefly Host Dashboard pushes the appropriate security policy to the Firefly Host VM which, in turn, inserts it into the Firefly Host Module.

- The Firefly Host Module

Virtualized network traffic is secured and analyzed against the security policy for all VMs on the ESX/ESXi host in the Firefly Host Module installed on the host. All connections are processed and firewall security is enforced in the Firefly Host module.

Related Documentation

- [Understanding the Firefly Host Architecture on page 4](#)
- [Understanding Cloud Computing and Firefly Host on page 6](#)

- [Understanding Hypervisors and Firefly Host on page 9](#)
- [Understanding the VMware Infrastructure and Firefly Host on page 7](#)
- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host VM on page 24](#)
- [Firefly Host Prerequisites and Resource Requirements for the VMware Environment on page 39](#)

Understanding the Firefly Host Architecture

Firefly Host is a fault-tolerant service provider and enterprise grade security solution that is purpose-built for the virtualized environment. Not only does it secure virtual machines (VMs), but it also protects the hypervisor. When it is deployed into the VMware environment and the Firefly Host VM is installed on a VMware ESX/ESXi host, the Firefly Host module (Firefly Host engine) is loaded into the host's hypervisor between the virtual network installation card (vNIC) and the virtual switch (vSwitch). The VMware VMsafe module gives Firefly Host full protocol inspection of every VM.

Firefly Host does not depend on the virtual switching layers for its oversight of VMs. Consequently, whichever vSwitch is used has no bearing on Firefly Host. It is compatible with them all.



NOTE: VMware lets you create abstracted network devices called virtual switches (vSwitches). A vSwitch routes traffic internally between virtual machines and external networks. A vSwitch can be connected to physical switches.

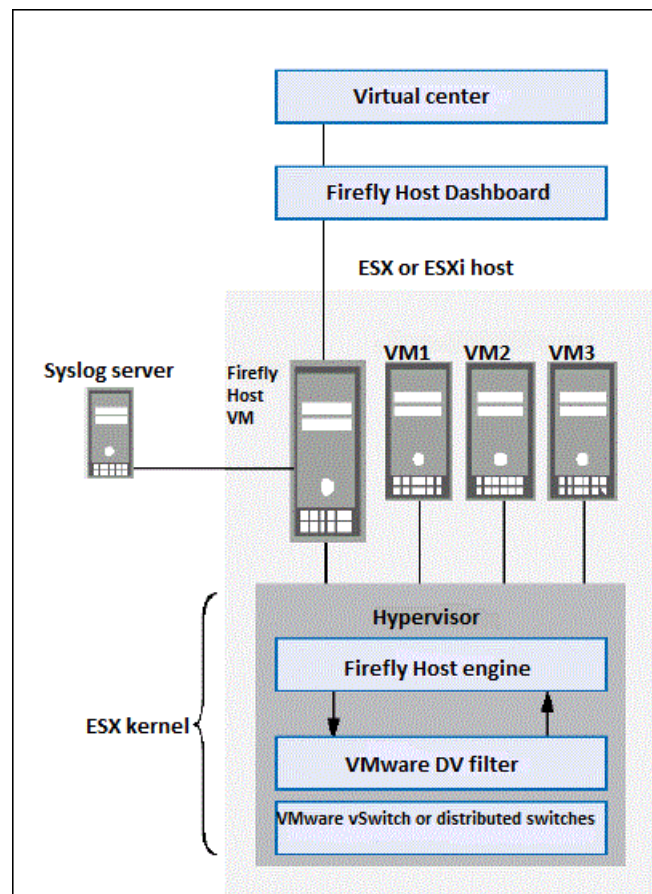
In the VMware virtualized environment, port groups are used to aggregate multiple ports under a common configuration. They serve as an anchor point for virtual machines that connect to labeled networks.

The Firefly Host Dashboard makes configuration changes in the VMware vCenter automatically. This lowers administrative complexity and reduces the possibility of configuration errors. [Figure 1 on page 5](#) shows the Firefly Host integration with VMware ESX/ESXi hosts and vCenter. [Figure 1 on page 5](#) also shows that:

- The Firefly Host Dashboard is integrated and communicating with the VMware vCenter. It is also communicating with the Firefly Host VM installed on the ESX/ESXi host.
- The Firefly Host VM, which is installed on the host, has inserted the Firefly Host engine (the Firefly Host Module) into the ESX/ESXi host's hypervisor.

From within the ESX/ESXi host's hypervisor, the Firefly Host engine is aware of all network connections between VMs on the host, coming into and going out to other hosts in the virtualized environment, and transiting the physical switch.

Figure 1: Firefly Host Architecture



Related Documentation

- [Firefly Host Installation and Upgrade Guide for VMware](#)
- [Firefly Host Administration Guide for VMware](#)
- [Firefly Host Getting Started Guide for VMware](#)
- [Configuring Firefly Host to Send Syslog and Netflow Data to Juniper Networks STRM Series Devices](#)
- [Installing an Additional Firefly Host Dashboard and Configuring the Primary Firefly Host Dashboard to Use It for High Availability](#)
- [Installing a Secondary Firefly Host VM for High Availability](#)
- [Integrating the Firefly Host with VMware Using the Settings Module](#)
- [Preparing to Integrate Firefly Host with the VMware Environment on page 43](#)
- [Understanding Hypervisors and Firefly Host on page 9](#)
- [Understanding the Firefly Host VM on page 24](#)
- [Understanding the Firefly Host High Availability Solution](#)
- [Understanding the Firefly Host Hypervisor and Extended VM Security](#)

- *Understanding Firefly Host Fault Tolerance Support*
- *Viewing the Firefly Host Logs*

Understanding Cloud Computing and Firefly Host

A cloud is an Internet-based environment of virtualized computing resources including servers, software, and applications that can be accessed by individuals or businesses with Internet connectivity. Customers, referred to as tenants, can access the resources that they need to run their businesses.

Clouds possess the following advantages. They:

- Allow customers to share the same infrastructure to gain price and performance advantages.
- Provide customers with a pay-as-you-go lease-style investment versus buying all of the required hardware and software up front themselves.
- Allow businesses to scale easily and tier more services and functionality on an as-needed basis.

There are two kinds of clouds and a third one that combines the other two:

- Public clouds

They are based on a standard cloud computing model. In this structure, a service provider (SP) hosting the cloud makes resources such as applications, computing capacity, storage, and server-based infrastructure available to the public.

The SP hosting the cloud owns and operates the infrastructure and offers access through the Internet.

- Private clouds

They are proprietary network or data center that use cloud computing technologies such as virtualization.

The infrastructure is operated solely for a single organization whether managed internally or externally. The company still must buy, build, and manage the infrastructure. It does not benefit from the economic gains offered by public cloud computing.

- Hybrid clouds

They are composed of two or more clouds that remain unique but are bound together providing benefits of multiple deployment models. They are maintained by both internal and external providers.

Hybrid clouds require both on-premises resources and off-site, remote server-based cloud infrastructure.

Cloud computing allows for dynamic and elastic generation of virtual infrastructure and virtual machines (VMs) with their own operating systems running over that infrastructure.

Whether for public, private, or hybrid clouds, virtualized data centers must offer secure, discrete, VM environments to their customers and their organizations.

Physical network security is designed for and limited to physical hardware and its software. It does not have the visibility into traffic transmission and communication between VMs that is required to secure the environment. Firefly Host secures the virtual network in ways that physical security mechanisms protecting physical networks cannot because it is purpose-built for virtualized environments. Firefly Host provides support for IPv6 in addition to IPv4 to enable organizations that have adopted IPv6 to benefit from Firefly Host cloud security.

**Related
Documentation**

- [Understanding Firefly Host on page 3](#)
- [Understanding Hypervisors and Firefly Host on page 9](#)

Understanding the VMware Infrastructure and Firefly Host

The Juniper Networks Firefly Host runs as integrated software on VMware vSphere servers.

This topic includes the following sections:

- [Understanding vSphere and the Firefly Host on page 7](#)
- [Understanding VMware ESX and ESXi Hosts and the Firefly Host on page 7](#)
- [Understanding VMotion and Firefly Host on page 8](#)

Understanding vSphere and the Firefly Host

VMware vSphere is a cloud operating system that can manage large pools of virtualized computing infrastructure, including software and hardware. Firefly Host components integrate with the VMware vSphere infrastructure to provide security for ESX/ESXi hosts in the virtualized environment. Because the Firefly Host is purpose-built to support virtualization, it synchronizes automatically with the VMware vCenter. It uses VMware's *VMsafe* interfaces to provide breakthrough levels of security and performance.



NOTE: Beginning with vGW Series 5.0r2, Firefly Host provides support for vSphere 5.0.

Understanding VMware ESX and ESXi Hosts and the Firefly Host

VMware ESX and ESXi hosts provide the foundation for building and managing a virtualized IT environment. These hypervisor-based hosts contain abstract processors, memory, storage, and networking resources that are shared among multiple virtual machines (VMs) that run unmodified, diverse operating systems and applications.

Firefly Host manages and secures the VMs that run on ESX/ESXi hosts.

The number of IP addresses or VMs that Firefly Host can protect is not determined. In any case, a single Firefly Host Dashboard management center can handle hundreds of hosts and their associated Firefly Host VMs, and each Firefly Host VM can load thousands

of policy rules. However, a Firefly Host VM loads only the policy rules that are relevant for the VMs which exist on the host where it resides. You can easily extend the reach of protection for your virtualized environment, if it is exceedingly large, by using the Firefly Host Split Center and Multi-Center features, which allow you to scale to accommodate any size requirements.

Understanding VMotion and Firefly Host

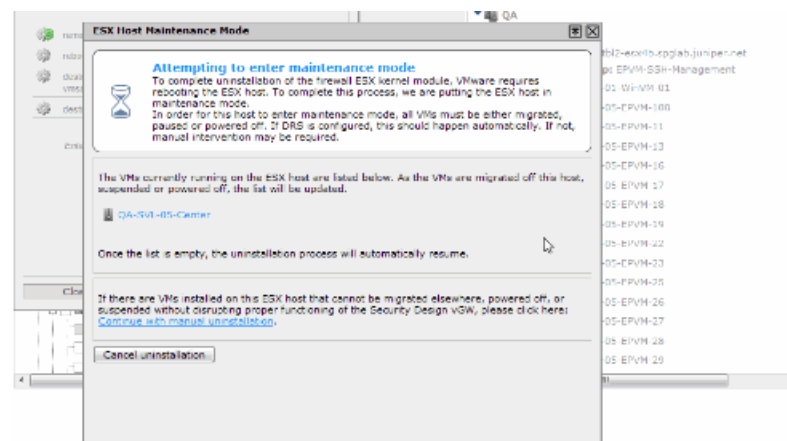
VMware provides a feature called *VMotion* that allows for transition of active, or live, VMs from one physical server to another. VMs can be moved from one server to another to perform maintenance operations on a host. Also, they can be moved automatically when VMotion is triggered through VMware's Dynamic Resource Scheduler (DRS), which is used to evenly distribute system resource usage across physical servers.

Because VMs can be migrated between servers, their security levels can be compromised and lowered from that of the original server to that of the new one. A VM could be migrated to an unsecured zone or one with a lower trust level.

Migration problems can ensue if your virtualized environment is configured to support both DRS and Firefly Host Dashboard VM offline updates. (Normally offline updates can be performed when the Firefly Host Dashboard VM is connected through the CD/DVD drive to an ISO image file on the local disk.) Given a configuration to support DRS and Firefly Host Dashboard VM offline updates, the migration process halts when it attempts to uninstall the Firefly Host VM from the ESX/ESXi host that contains the connected Firefly Host Dashboard VM and the Firefly Host VM migration does not occur.

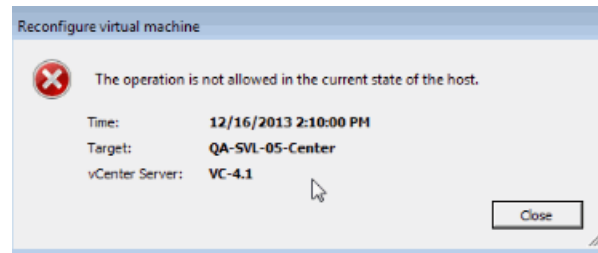
During the Firefly Host Dashboard VM install/uninstall task after the process enters maintenance mode the pop up box shown in [Figure 2 on page 8](#) is displayed to identify the VMs that are running on the ESX/ESXi host. As VMs are powered off, suspended, or migrated from the ESX/ESXi host, they are removed from the list. Given the configuration described in this issue, the pop up box display activity halts when the task encounters the Firefly Host VM.

Figure 2: Pop-Up Box Displayed During Firefly Host VM install/un-install Process



To solve the problem and allow the process to continue, you must disconnect in vSphere the CD/DVD drive from the Firefly Host Dashboard VM. At the point where the task is halted, the pop up box displays the message shown in [Figure 3 on page 9](#) directing you to use the vSphere toolbar to disconnect the CD/DVD. After the CD/DVD drive is disconnected, the migration process is resumed.

Figure 3: Problem Resolution Message for vMotion Halt



VMs can be moved from one server to another to perform maintenance operations on an ESX/ESXi host. VMware's Dynamic Resource Scheduler (DRS) can trigger vMotion, which causes automatic transition of live VMs from one physical server to another.

Unlike traditional firewalls, the Firefly Host firewall supports live migration by maintaining open connections and security throughout the event. Firefly Host ensures that appropriate security for a VM remains intact throughout migration.

Related Documentation

- [Preparing to Integrate Firefly Host with the VMware Environment on page 43](#)
- [Firefly Host VMsafe Firewall + Monitoring and VMsafe Monitoring Modes on page 44](#)
- [Understanding Firefly Host Environment Time Synchronization on page 44](#)
- [Understanding the Open Virtualization Format OVA Template Method on page 47](#)
- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 48](#)
- [Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware on page 56](#)
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 58](#)
- [Setting Up Firefly Host on page 61](#)

Understanding Hypervisors and Firefly Host

Firefly Host is a high performance, hypervisor-based virtualization security solution. Various layers of abstraction combine to create virtualized environments. Virtualized hardware supports multi-tenancy in which guest virtual machines (VMs) running discrete operating system images share the system resources. Each guest VM runs its own user-space applications. If a physical machine does not directly support virtualization, a software layer called a hypervisor is used to manage the relationship between the guest VMs that run on it and compete for its resources.

Some forms of virtualization provide support for multiple instances of only the same kind of guest operating system. A full-virtualization hypervisor allows multiple instances of a *variety* of guest operating systems to run concurrently. It presents a virtual operating platform to the guest operating systems, and it manages their execution. Similar to the control program responsibilities of the supervisor that is intrinsic to some operating systems, a full-virtualization hypervisor arbitrates access to resources between guest VMs that reside on the host and it manages those guest VM operating systems.

Firefly Host secures full virtualized environments by inserting a module into the hypervisor of the host. Because the Firefly Host Module resides in the hypervisor, Firefly Host has wide visibility into the virtualized environment, and it can process security requirements and traffic protection fast and reliably.

**Related
Documentation**

- [Understanding Firefly Host on page 3](#)
- [Understanding Cloud Computing and Firefly Host on page 6](#)
- [Understanding IPv6 Addressing](#)

CHAPTER 2

Firefly Host Dashboard and Firefly Host VM

- [Understanding the Firefly Host Dashboard on page 11](#)
- [Firefly Host Dashboard Modules \(VMware\) on page 12](#)
- [Understanding the Firefly Host Main Module on page 17](#)
- [Understanding the Firefly Host VM on page 24](#)
- [Understanding the Firefly Host Module on page 24](#)

Understanding the Firefly Host Dashboard

Firefly Host includes a management center vm, with a graphical user interface (GUI) called the Firefly Host Dashboard. The Firefly Host Dashboard allows you to create multi-tiered policies to protect and secure VMs. You use it to push those policies to Firefly Host VMs which are installed on the hosts that they secure.

The Firefly Host Dashboard modules provide features that allow you to perform the following tasks and many others:

- Perform network traffic analysis.
- Configure your environment to protect against intrusions and attacks.
- Quarantine suspect files and VMs.
- Inspect for malware and anomalous behavior.
- Configure and generate reports providing information on all aspects of your monitored and secured environment.
- Create dynamic groups called Smart Groups that secure VMs automatically in various ways based on characteristics of the VM without your needing to intervene.

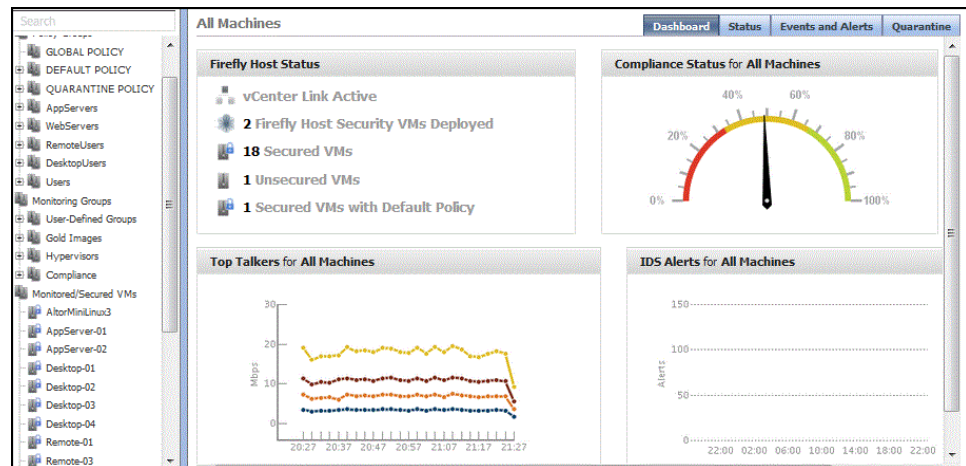
You use the Firefly Host Dashboard to configure Firefly Host. You must use a Web interface browser to access the Firefly Host Dashboard by its IP address. You can obtain the IP address by clicking the **Summary** tab of the Firefly Host Dashboard.

After you initially bring up the Firefly Host Dashboard, you can access it by entering **admin** for the username and entering the password that was set during installation. To log out

of the Firefly Host Dashboard, click **logout** in the upper right corner of the Firefly Host Dashboard page.

When you log in to the Firefly Host Dashboard, you see the Main module page with its Dashboard tab. See [Figure 4 on page 12](#). The page displays information gathered from the activity of various Firefly Host Dashboard modules.

Figure 4: Main Module Displayed at Login



Related Documentation

- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [About the Firefly Host Dashboard Tree on page 30](#)
- [Understanding Firefly Host Dashboard Navigation on page 27](#)

Firefly Host Dashboard Modules (VMware)

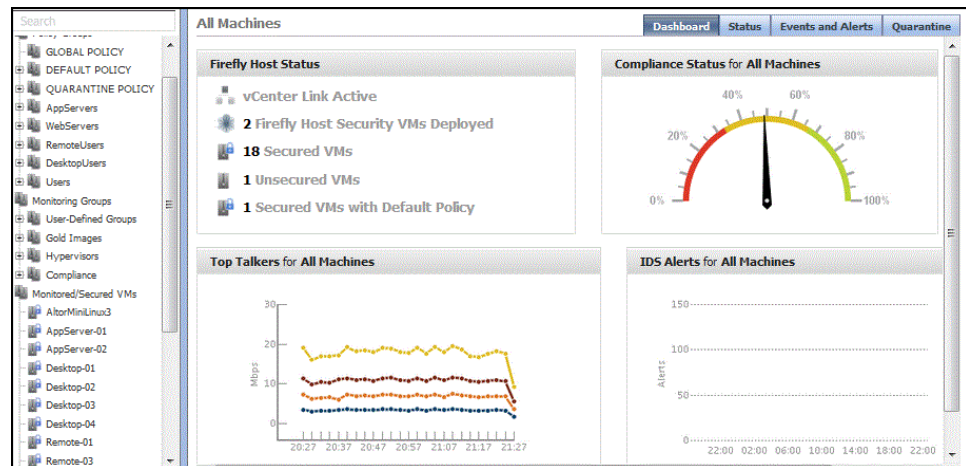
The Firefly Host Dashboard is composed of the following modules that implement Firefly Host features:

- Main
- Network
- Firewall
- IDS
- AntiVirus
- Introspection
- Compliance
- Reports
- Settings

The following figures show the modules' primary pages. A link is provided to the section that covers the module. The highlighted button on the taskbar at the top of the page indicates the active feature.

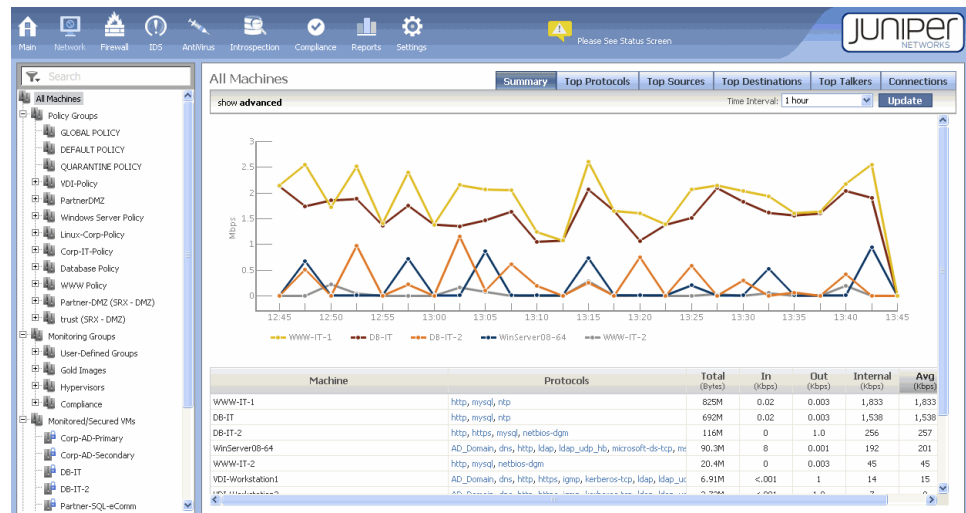
- Main. See [“Understanding the Firefly Host Main Module” on page 17](#) and [Figure 5 on page 13](#).

Figure 5: Main Module



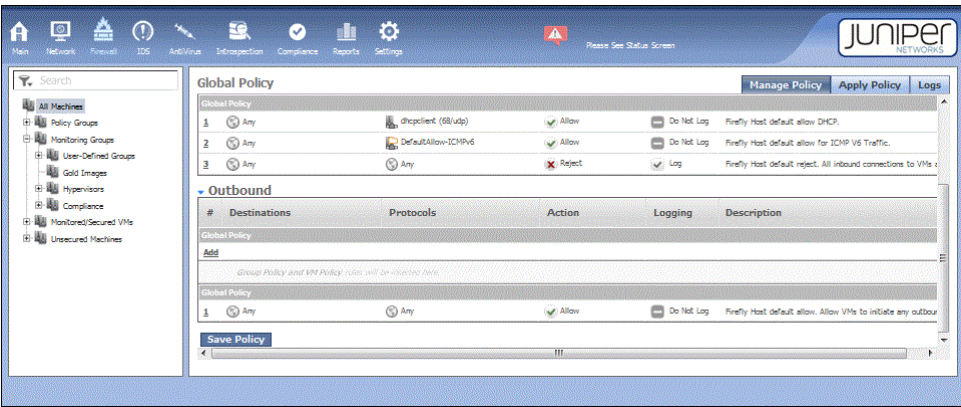
- Network. See [Understanding the Firefly Host Network Module](#) and [Figure 6 on page 13](#).

Figure 6: Network Module



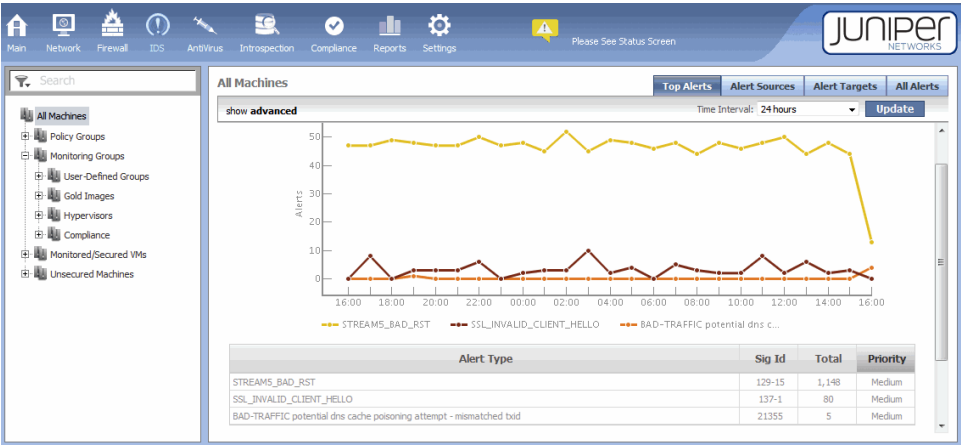
- Firewall. See [Understanding the Firefly Host Firewall Module](#). See [Figure 7 on page 14](#).

Figure 7: Firewall Module



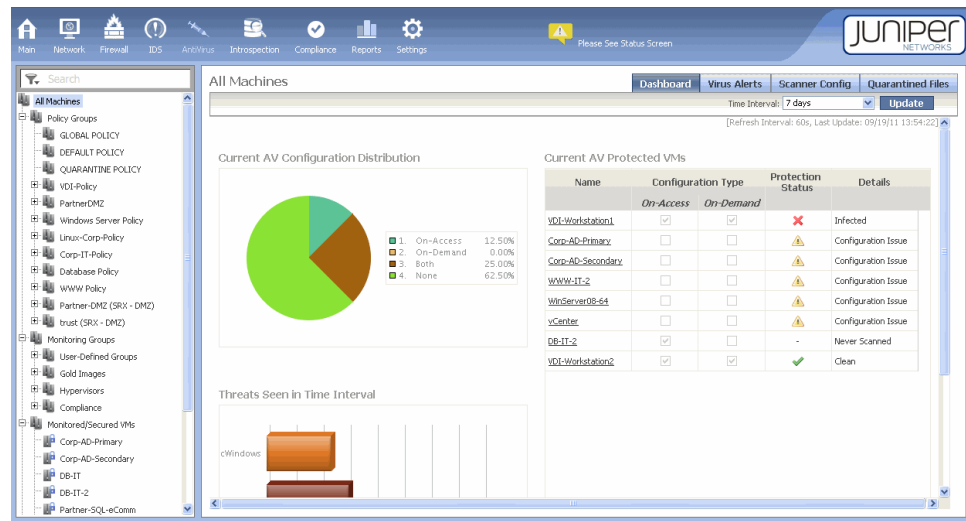
- IDS. See Understanding the Firefly Host IDS Module and [Figure 8 on page 14](#).

Figure 8: IDS Module



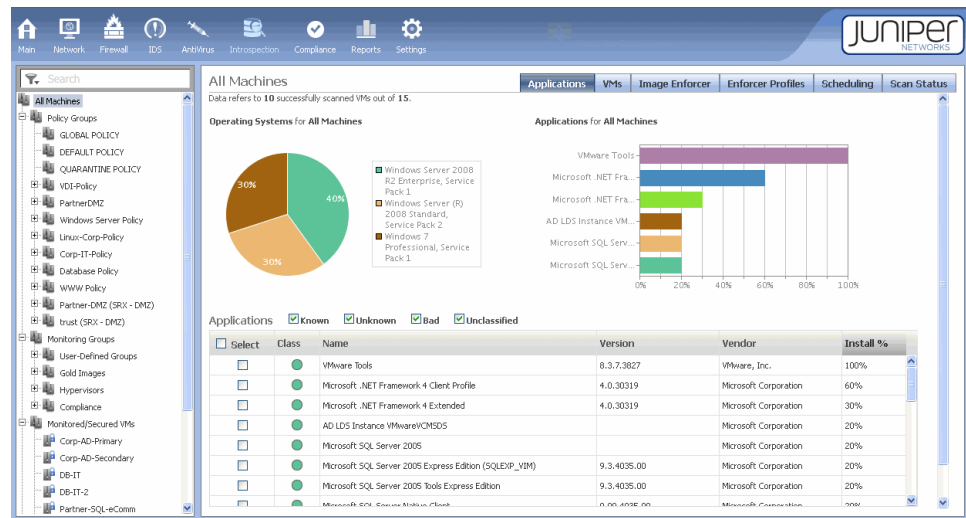
- AntiVirus. See Understanding Firefly Host AntiVirus and [Figure 9 on page 15](#).

Figure 9: AntiVirus Module



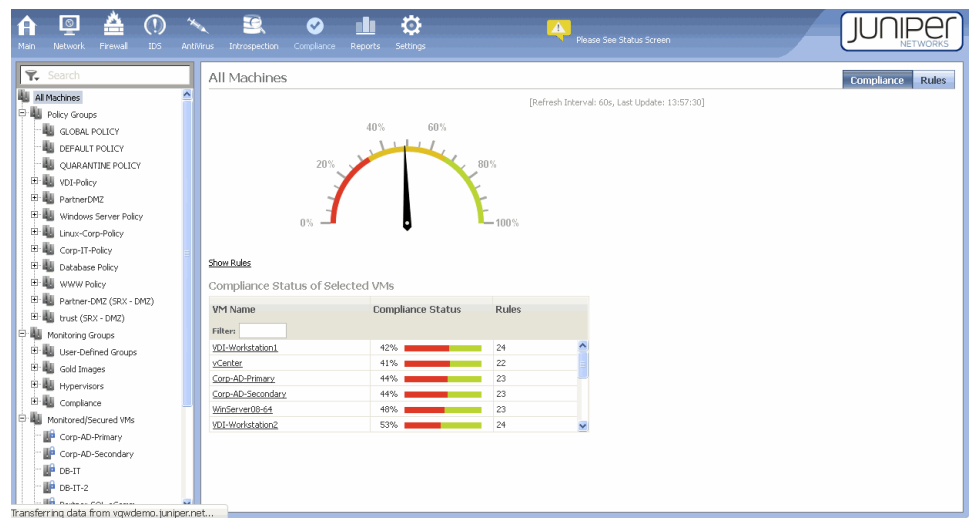
- **Introspection.** See Understanding the Firefly Host Introspection Module and [Figure 10 on page 15](#).

Figure 10: Introspection Module



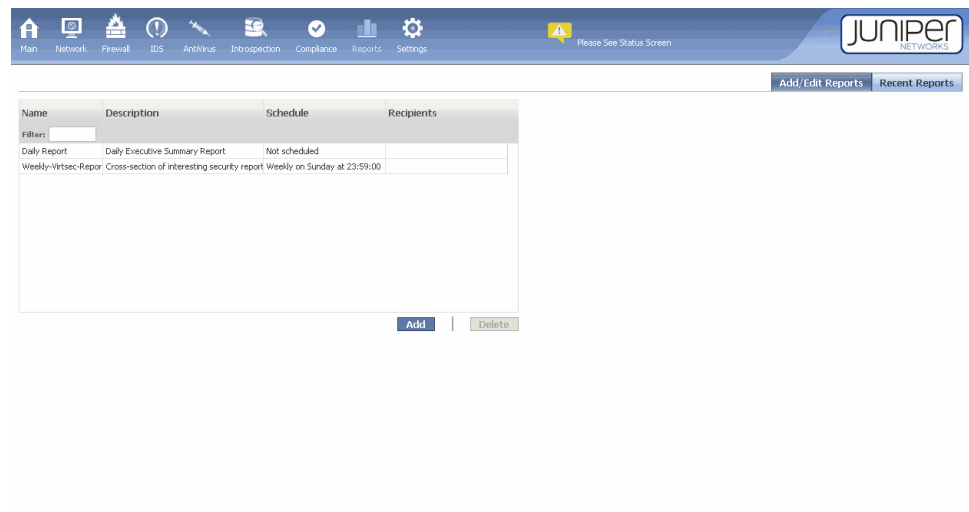
- **Compliance.** See Understanding the Firefly Host Compliance Module and [Figure 11 on page 16](#).

Figure 11: Compliance Module



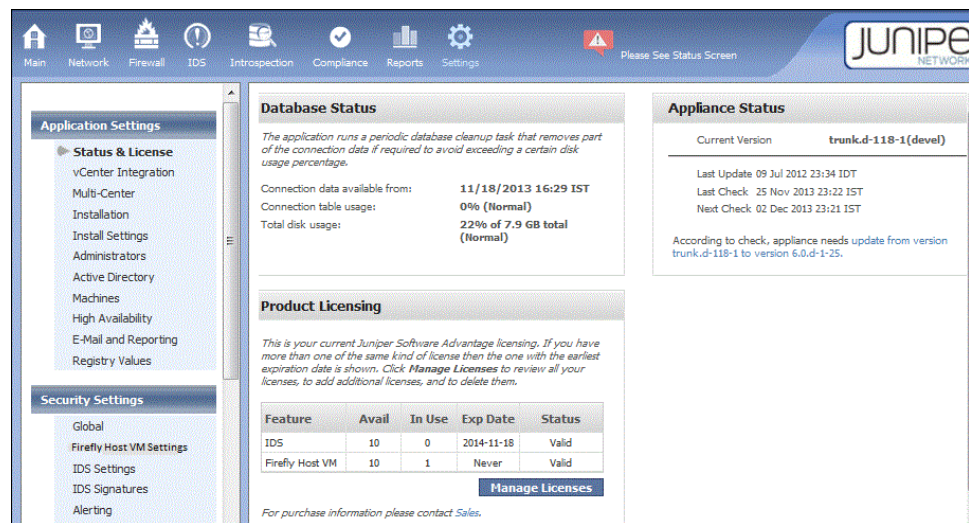
- Reports. See Understanding the Firefly Host Reports Module and [Figure 12 on page 16](#).

Figure 12: Reports Module



- Settings. See Understanding the Firefly Host Settings Module and [Figure 13 on page 17](#).

Figure 13: Settings Module



Related Documentation

- [Understanding the Firefly Host Main Module on page 17](#)
- [Understanding the Firefly Host Module on page 24](#)
- [Understanding the Firefly Host VM on page 24](#)
- [Understanding Firefly Host Status and Alerts on page 35](#)

Understanding the Firefly Host Main Module

The Main module of the Firefly Host Dashboard displays information gathered from many of the Firefly Host Dashboard components. When Firefly Host detects new events and alerts, data and graphs in the Main module's panes are automatically refreshed.

The Main module contains the following tabs.

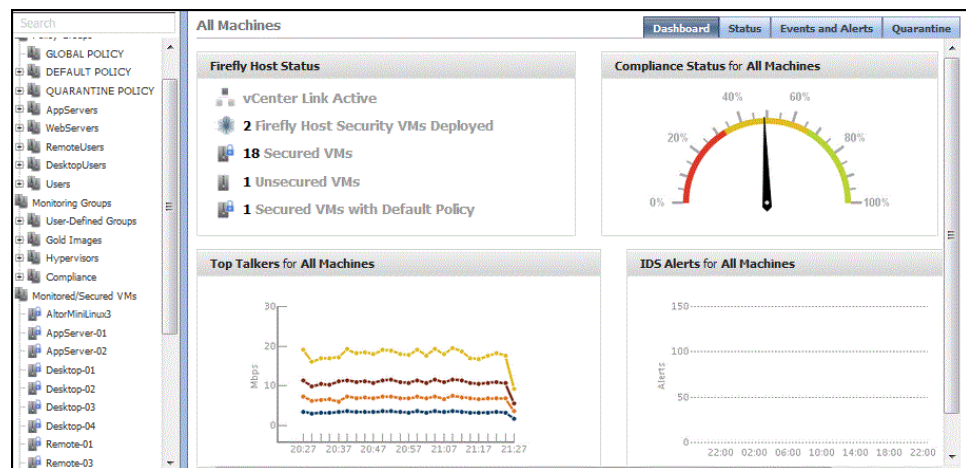
- [Dashboard on page 17](#)
- [Status Tab on page 18](#)
- [Events and Alerts Tab on page 20](#)
- [Quarantine Tab on page 23](#)

Dashboard

In both graphical and table format, the Dashboard allows you to view the behavior of your environment at a glance. You can view the activity of all virtual machines (VMs). You can select an individual VM or a group of VMs in the VM tree to focus on. The Dashboard displays information for both IPv4 and IPv6 traffic.

See [Figure 14 on page 18](#).

Figure 14: Dashboard Tab



The Dashboard includes the following panes:

Firefly Host Status—Provides an overview of the current state of your infrastructure. It shows the state of Firefly Host connectivity to the VMware vCenter. It also shows the number of Firefly Host VMs deployed to secure ESX/ESXi hosts, and the overall state of your deployment's VMs, that is, whether they are secured by Firefly Host or not.

Compliance Status for All Machines—Shows the overall posture of all VMs in your organization that might be violating compliance rules. The more VMs that violate rules (high weighting), the further the needle moves to the red.

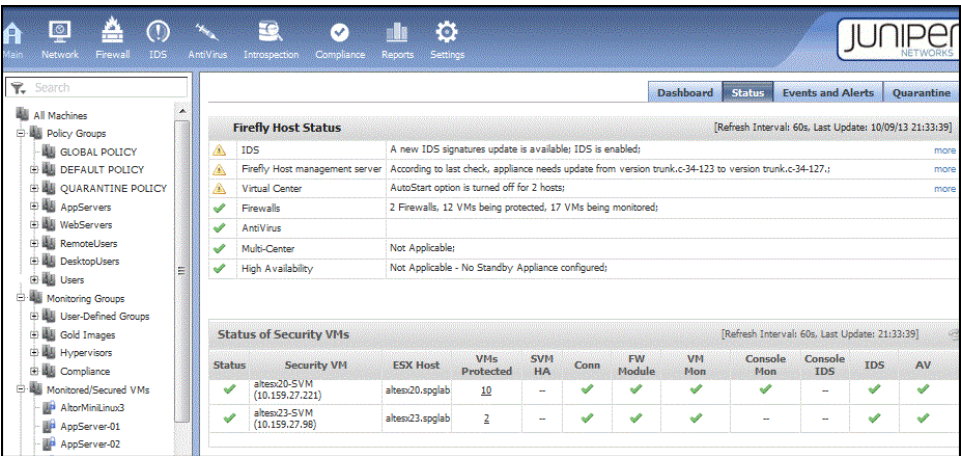
Top Talkers for All Machines —Displays network activity for the last hour.

IDS Alerts for All Machines—If IDS is enabled, the overall IDS alerts information is displayed.

Status Tab

The Status tab displays a summary of Firefly Host settings for each module, and it displays status on individual Firefly Host VMs. The page is refreshed every 60 seconds. See [Figure 15 on page 19](#).

Figure 15: Status Tab



NOTE: For Firefly Host VMs for which standby or secondary Firefly Host VM instances are configured, Firefly Host counts only the primary Firefly Host VM and reflects that count in the Firefly Host Status table Firewalls number.

For disconnected Firefly Host VMs, Firewalls shows separate counts for primary, standby, and secondary Firefly Host VMs. For example, it might show “1 disconnected, 1 Standby disconnected, 1 Secondary disconnected”.

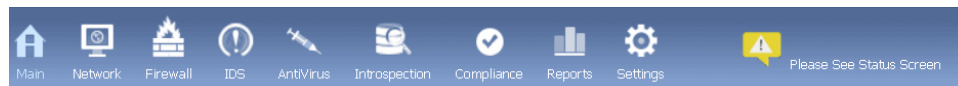
The Status page includes these panes:

Firefly Host Status—For the Firefly Host components, the pane indicates the current state using the status icons shown in Table 3 on page 19.

Table 3: Firefly Host Status Icons

Icon	Indicates
	Firefly Host component is working properly.
	One or more issues exist with the component. For example, maintenance settings might be incompatible or disabled, or you might need to update its firewall.
	Significant issues exist for the component. For example, a module did not load correctly.

In addition to these icons, an overall health status icon appears when individual components require your attention. Figure 16 on page 20 shows the taskbar with the health status icon at the far right. The icon is either red or yellow, depending on the underlying state of the components being monitored.

Figure 16: Taskbar Showing the Health Status Icon

Status of Firefly Host VMs—This pane reports status on individual Firefly Host VMs.

This pane shows the following information:

- Firefly Host VM name.
- Host that the Firefly Host VM protects.
- Number of VMs that it protects.

For Firefly Host VMs configured with secondary or standby instances, Firefly Host counts VMs protected by the primary Firefly Host VM. That is, it does not count the same VM again in relation to the secondary or the standby Firefly Host VM instance.

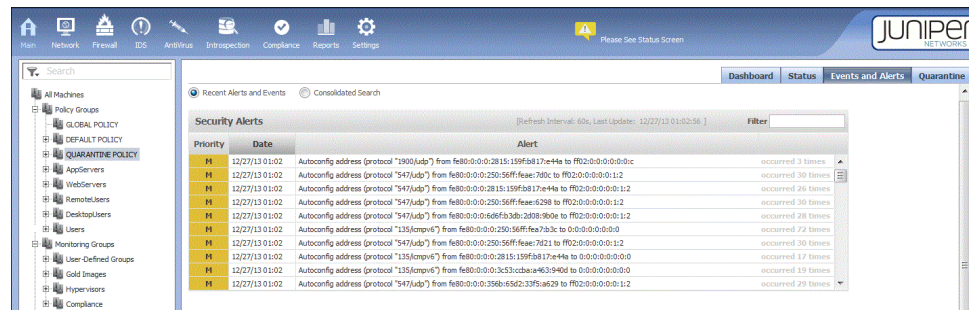
- If Firefly Host HA is enabled.
- If the Firefly Host VM is connected to the Firefly Host Dashboard.
- If the firewall module is enabled.
- If VM monitoring is used.
- IP address of the Firefly Host Dashboard management center.
- If IDS is used, the IP address of the IDS console.
- If IDS is enabled, IDS data appears. Otherwise, the chart is blank.
- If AntiVirus is enabled.

Click the Status icon for a Firefly Host VM to display detailed information about it. When you click the icon, the Firefly Host Dashboard automatically positions you in the Firefly Host Settings section of the Settings module that pertains to the selected Firefly Host VM. You can use the tabs on that page to change configuration settings for the Firefly Host VM. See *Understanding the Firefly Host VM Settings*.

Events and Alerts Tab

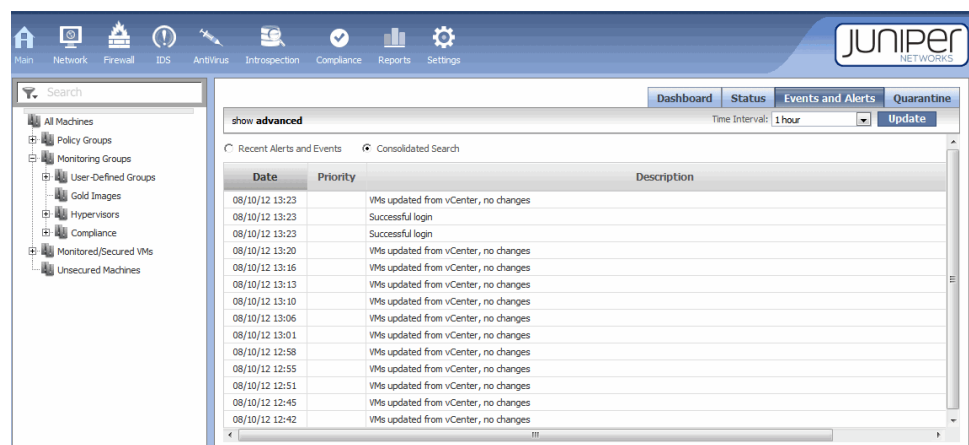
The Events and Alerts page allows you to view Security Alerts and System Status and Events messages individually, in separate panes of the page. You can use an individual filter to search each set separately. See [Figure 17 on page 21](#).

Figure 17: Main Module Events and Alerts Page



Alternatively, you can search through the combined logs for a specific time period using the Consolidated Search button. For example, you might want to look at historical data. Rather than searching through each set, you can specify a time and see all the logs for that period. See [Figure 18 on page 21](#).

Figure 18: Consolidated Logs for Events and Alerts



- [Security Alerts on page 21](#)
- [System Status and Events on page 22](#)

Security Alerts

The Security Alerts pane lists all Firefly Host alerts that have occurred in your protected virtualized environment, except for IDS alerts and AntiVirus alerts which are reported in their own modules. The reported alerts are primarily Firefly Host system-related events, such as reports on occurrences of Firefly Host version updates or alerts when component failures occur.

Alerts are classified as high (H), medium (M), or low (L), depending on their severity. Click the **Priority** or **Date** column to sort the list differently. You can use the filter to sort the data by IPv6 or IPv4 address. The pane will show the alert or event for only the VM with the IP address that you enter.

System Status and Events

Many companies require a complete audit trail of administrative and policy operations to meet compliance standards and their security best practices. A detailed audit trail is an important part of a security infrastructure that security administrators rely on.

Firefly Host collects information on events and posts it to the System Status and Events pane when administrative and policy operations occur. It posts the following event alerts:

- An administrator logs in or logs out, and when failed login attempts occur
- An administrator changes Firefly Host Dashboard settings, including the following:
 - Changes to general system settings such as log connections, system reboots, and active directory
 - Manual VM updates
 - Modifications to Firefly Host objects, including networks, machines, groups, protocols, an administrator settings
 - Updates to the Firefly Host Dashboard
 - Updates to the Firefly Host VM
 - Configuration changes to firewall
 - Configuration changes to Syslog, Netflow, external inspection devices, and infrastructure reinforcement
- Automatically secured VM configuration changes occur
- IDS signatures are modified and new signatures are added
- Introspection scans are started on **Scan Now** requests, scheduled events occur, and scheduled scan configurations are modified
- Compliance Rule modifications are made
- Reports are created or Reports configuration settings are modified
- The Image Enforcer is configured, its configuration settings are changed, and Image Enforcer scans occur
- AntiVirus is configured, changes are made to its configuration, and AntiVirus scans occur
- SRX Series integration changes take place
- Multi-Center and Split-Center settings are configured or changed.
- Backup and Restore is configured and when configuration changes are made
- Registry values are changed

Events are listed chronologically. The events that occurred most recently are listed at the top of the table. To view additional events, you can access the Firefly Host Dashboard database.

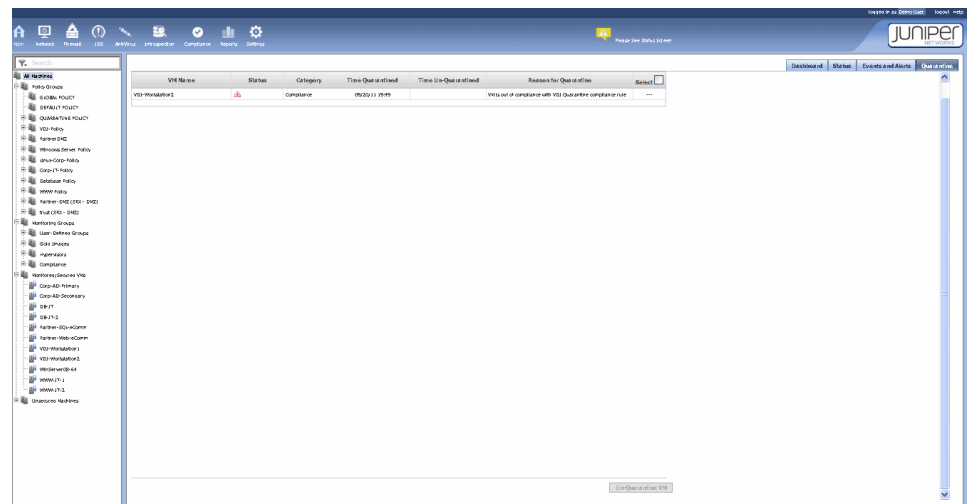
You can configure the Alerting pane in the Settings module to allow alerts to be sent also to administrators through e-mail. See *Firefly Host Event and Alert Messages Guide Reference*.

You can use the filter to sort the data, including by IPv6 or IPv4 address. For example, you can enter the IPv6 address of a specific VM and see only the alerts and events for it.

Quarantine Tab

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. You can also remove a VM from quarantine from this page. See [Figure 19 on page 23](#).

Figure 19: Quarantine Tab



To display information about quarantined VMs for one or more features, select the check box beside the feature. You can view information about VMs quarantined as a result of only one type of scan or you can view all information for any of them in combination. For any of these selections you can display:

- Information about currently quarantined VMs.
- Historical information about previously quarantined VMs.

The Quarantine page shows the following information for each VM:

- Status
- Category
- Time quarantined
- Time un-quarantined.
- Reason why the VM was quarantined.

To remove a VM from quarantine, check the select box for it and click **Un-Quarantine VM**.



NOTE: You can use the AntiVirus module to quarantine files infected by a virus or other malware. See *Understanding Firefly Host AntiVirus*.

For details on the relationship between the Main module Quarantine tab, the Quarantine Policy group, and AntiVirus, Compliance, and Image Enforcer scans, see *Understanding Quarantined VMs and How to Manage Them*.

**Related
Documentation**

- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [About the Firefly Host Dashboard Tree on page 30](#)
- [Understanding Firefly Host on page 3](#)

Understanding the Firefly Host VM

To secure the virtual machines (VMs) on an ESX/ESXi host, you install a Firefly Host VM on the host. In turn, the Firefly Host VM installs the Firefly Host Module into the VMware hypervisor of the host. The Firefly Host VM acts as a conduit between the Firefly Host Dashboard and the Firefly Host Module. The Firefly Host VM also maintains policy and logging information.

You use the Firefly Host Dashboard to deploy Firefly Host VMs to ESX/ESXi hosts. You use it to create firewall policies that are pushed to the Firefly Host VMs. The Firefly Host VM inserts the policies into the Firefly Host Module where all connection enforcement occurs.

**Related
Documentation**

- [Understanding the Firefly Host VM Settings](#)
- [Understanding the Firefly Host Firewall Module on page 79](#)
- [Installing Firefly Host VMs on ESX/ESXi Hosts](#)
- [Installing a Secondary Firefly Host VM for High Availability](#)

Understanding the Firefly Host Module

Firefly Host Module is the policy enforcement engine that is loaded into the hypervisor of an ESX/ESXi host to be secured. It utilizes the VMware VMID to ensure that the correct policy is applied to a VM. It manages state synchronization in order to support VMotion.

It is a lightweight component that plugs directly into the host's hypervisor—without relying on an OS or a VM.

Communication between the Firefly Host Module in the ESX/ESXi host's hypervisor and the Firefly Host VM occurs over a special VMware vmservice vSwitch.

Firefly Host VM is the conduit to the Firefly Host Module. It inserts security policy into the Firefly Host module, transfers logs and network information from the Firefly Host module to the Firefly Host Dashboard and other devices SYSLOG, NetFlow V9 devices.

**Related
Documentation**

- [Understanding the Firefly Host VM on page 24](#)
- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host Dashboard on page 11](#)

CHAPTER 3

Firefly Host Dashboard Navigation and VM Tree

- [Understanding Firefly Host Dashboard Navigation on page 27](#)
- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [About the Firefly Host Dashboard Tree on page 30](#)

Understanding Firefly Host Dashboard Navigation

You use the Firefly Host Dashboard taskbar in conjunction with the VM tree to navigate the graphical user interface. The combination of the two allows you to select VMs and view and configure information about selected ones. See [Figure 20 on page 27](#) and [Figure 21 on page 28](#).

You can use the search field to filter VMs in various ways. See [“About the Firefly Host Dashboard Tree” on page 30](#).

Figure 20: Firefly Host Dashboard Taskbar

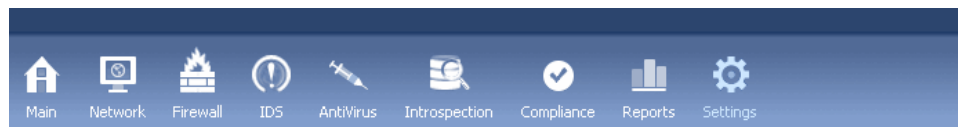
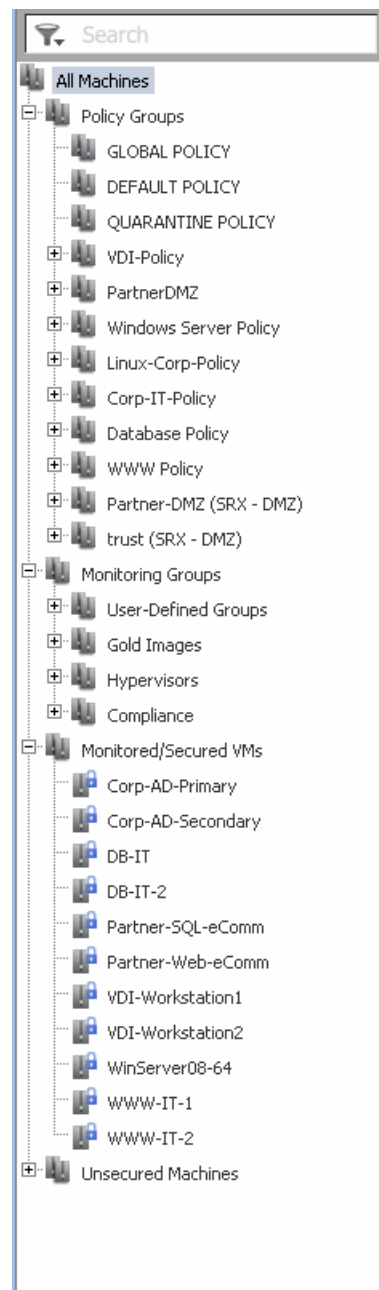


Figure 21: VM Tree



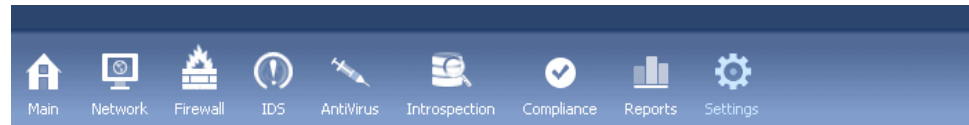
Related Documentation

- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [About the Firefly Host Dashboard Tree on page 30](#)
- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host Dashboard on page 11](#)

Understanding the Firefly Host Dashboard Taskbar

The taskbar lets you select the Firefly Host Dashboard module to use and move from one module to another. The Firefly Host Dashboard provides a modular configuration and information display structure. The taskbar includes icons representing the various modules. [Figure 22 on page 29](#) shows the taskbar.

Figure 22: Firefly Host Dashboard Taskbar



[Table 4 on page 29](#) identifies the modules that the Firefly Host Dashboard icons represent. You can click the link for a module to go to a topic that covers it.

Table 4: Taskbar Icons








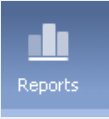

Icon	Module	Description	For details, see:
	Main	Combines status, alerts, and network activity into a single view. It identifies the VMs that are quarantined and allows you to take action on them.	“Understanding the Firefly Host Main Module” on page 17
	Network	Displays a network activity summary, top protocols, sources, destinations, talkers, and connections.	Understanding the Firefly Host Network Module
	Firewall	Manages and installs policies, and displays logs.	Understanding the Firefly Host Firewall Module
	IDS	Monitors all network traffic or a selected subset of VMs or protocols.	Understanding the Firefly Host IDS Module
	AntiVirus	Protects VMs by detecting malware, and it quarantines affected files or VMs.	Understanding Firefly Host AntiVirus

Table 4: Taskbar Icons (*continued*)

Icon	Module	Description	For details, see:
 Introspection	Introspection	Scans systems and reports on the software running in each VM (operating systems, patch-levels, and applications). It includes an Image Enforcer feature that allows you to specify VM templates or active VMs whose configurations are used as Gold Image comparison points. Contents of VMs are compared against the Gold Image.	Understanding the Firefly Host Introspection Module
 Compliance	Compliance	Monitors the virtual infrastructure against a predefined set of rules to guarantee all components are configured securely.	Understanding the Firefly Host Compliance Module
 Reports	Reports	Produces detailed system and security reports.	Understanding the Firefly Host Reports Module
 Settings	Settings	Controls configuration settings, including passwords.	Understanding the Firefly Host Settings Module

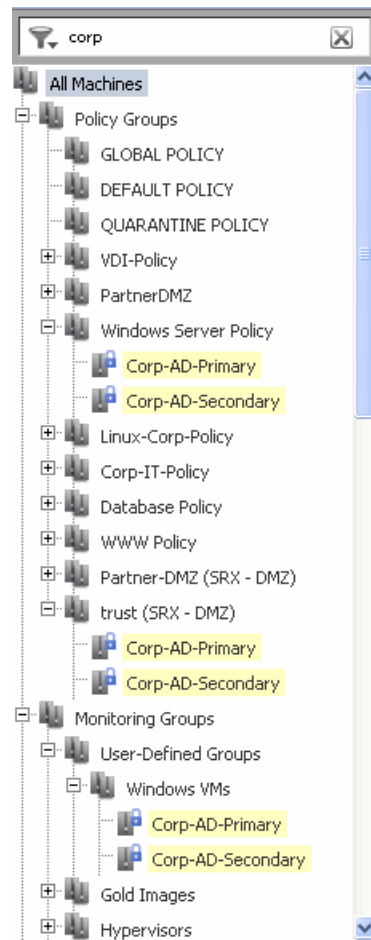
- Related Documentation**
- [About the Firefly Host Dashboard Tree on page 30](#)
 - [Understanding the Firefly Host Dashboard on page 11](#)
 - [Understanding Firefly Host on page 3](#)

About the Firefly Host Dashboard Tree

You use the VM tree in conjunction with the Firefly Host Dashboard modules. The VM tree lets you select virtual machines (VMs) to focus on, configure, and view information about.

You can select a group of VMs or an individual VM in the VM tree either by clicking its name or using the filter box. [Figure 23 on page 31](#) shows VMs belonging to three groups.

Figure 23: VM Tree with Selected VMs



See “Understanding the Firefly Host Dashboard Taskbar” on page 29.

- [VM Tree Overview on page 31](#)
- [Locating VMs in a Complex VM Tree on page 32](#)

VM Tree Overview

In conjunction with the selected Firefly Host Dashboard module, the VM tree controls the information displayed in the pane beside it. You can select all VMs in the tree, groups of VMs, or a single VM. When you select a module using the taskbar, that module's content appears as it applies to the VMs that you selected in the VM tree. The module controls the type of information that appears; the tree controls the VMs whose information appears. The combined selections allow you to configure or view information for that module as it pertains to the VMs. For example, to view network traffic for all machines, select **All Machines** in the tree, and then click the Network icon in the taskbar.

The VM tree contains the following main groups:

- Policy Groups

Contains all security policy groups, including Global, Default, and Quarantine. It also contains Illegal IPv4 Sources and Illegal IPv6 Sources groups and any policy groups that you define.

- Monitoring Groups

Contains all groups that were created with the Policy Group option, groups for monitoring the Hypervisor and Compliance state, and a group containing VMs or templates used as Gold Images by the Introspection module's Image Enforcer feature.

- Monitored/Secured VMs







Lists VMs monitored by the Firefly Host, VMs that have a firewall protecting their network traffic, or both.

- Unsecured Machines

Lists all VMs that are not currently being analyzed or protected by the Firefly Host.

[Table 5 on page 32](#) identifies the icons that show the state of monitored VMs.

Table 5: Virtual Machine State Icons

	The VM is being fully monitored, but it is not secured. For example, no firewall policy is loaded.
	The VM or the externally defined machine is not being monitored, and it has not been moved to a network secured by Firefly Host. NOTE: Network reports can display sessions between an unmonitored system and a monitored VM.
	Firefly Host cannot determine the IP address of the machine. This could be because it is powered down, suspended, or does not have VMware Tools installed. TIP: You can manually define an IP address by selecting the Settings module's Firefly Host Application Settings > Machines .
	The VMs are compliant.
	The VMs are not compliant.
	This is a VMware component. For example, it is an ESX/ESXi host.

Locating VMs in a Complex VM Tree

Locating VMs in the VM tree can become difficult as the VM tree grows in complexity. To simplify the process and make it easier to find specific VMs, the VM tree provides a

filter with advanced capabilities. You can enter in the filter box a text string that matches VM names within the tree. As you enter the text, the Firefly Host dynamically searches the tree for any matches.



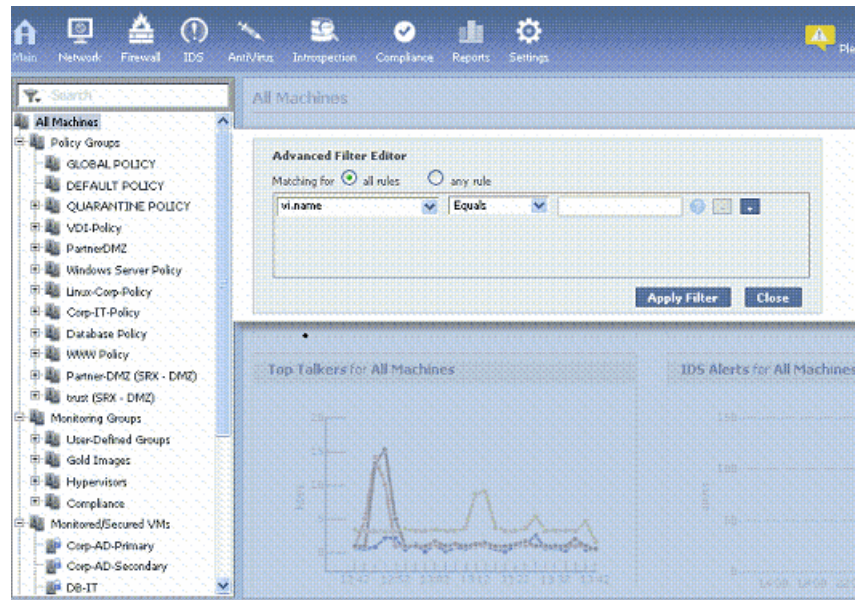
NOTE: An x icon is shown at the right side of the search field as the filter is being applied. You can use it to clear the filter.

As the filter is applied, the tree is expanded to show matching VMs. You do not need to expand all groups in the tree to find them. Branches in the tree that do not contain matches are collapsed.

You can use the Advanced Filter Editor feature to search the VM tree based on attributes rather than by name.

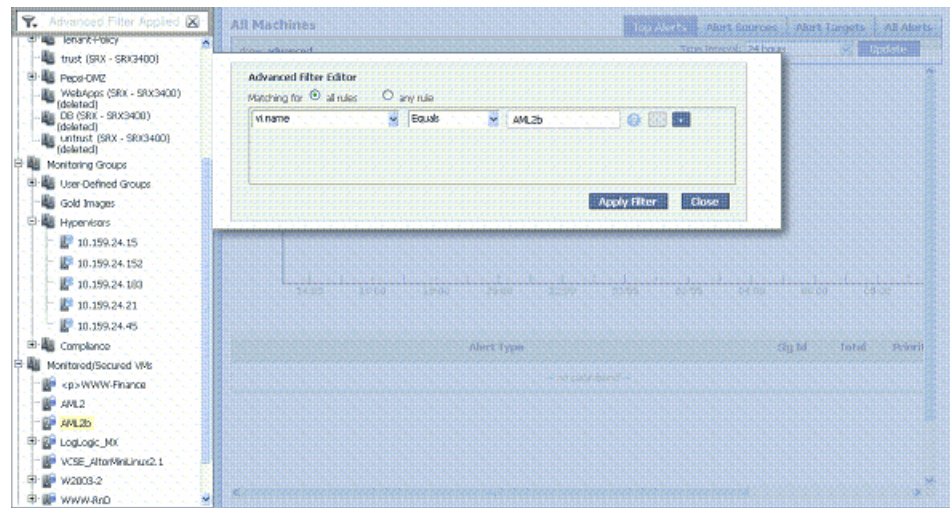
To use the advanced filter, click the icon at the left side of the search filter. This displays the Advanced Filter Editor shown in [Figure 24 on page 33](#).

Figure 24: Searching All VMs in the VM Tree Using the Advanced Editor



You can search based on data such as the portgroup, VLAN, and the IP protocol family using attributes such as `vi.portgroup`, `vi.vlan`, `vi.ipv4`, and `vi.ipv6`. You can also search for VMs by name. See [Figure 25 on page 34](#).

Figure 25: Searching for Specific VMs in the VM Tree Using the Advanced Editor



To remove the filter and collapse the branches, click the x icon to the right of the filter.

Related Documentation

- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [Understanding the Firefly Host VM on page 24](#)
- [Understanding Firefly Host on page 3](#)

CHAPTER 4

Status and Alerts

- [Understanding Firefly Host Status and Alerts on page 35](#)

Understanding Firefly Host Status and Alerts

Firefly Host can display several status icons within the user interface and several mechanisms for sending alerts, so that you know exactly what is happening on the virtual network.

- [Status on page 35](#)
- [Alerts on page 35](#)

Status

Firefly Host interface displays a yellow or red status icon to indicate an event or configuration issue that merits attention.

Click the status icon to display the Status tab in the Main module's page.

The sections of the product that have triggered a status change are displayed with most important status changes at the top shown in red. For details on the status issues, click the more link next to the status summary line.

Alerts

Firefly Host can send alerts when the log field in a rule in a security policy is set to Alert or Custom E-Mail Alert Tag and a connection matching this rule is seen on the network.

In addition to alerts generated by security rules, Firefly Host monitors High, Medium and Low Security events, displayed on the Main module's Events and Alerts tab, and it reports those Alerts out through the settings here (that is, through E-Mail, SNMP trap, or both).

In both cases, alerts use the settings found in Settings -> Security Settings -> Alerting.

You can choose to send an e-mail alert and an SNMP trap, only e-mail alerts, or only SNMP traps.

Related Documentation

- [Understanding Firefly Host on page 3](#)

PART 2

VMware and Firefly Host

- [Overview on page 39](#)
- [OVA and Firefly Host Deployment on page 47](#)

CHAPTER 5

Overview

- [Firefly Host Prerequisites and Resource Requirements for the VMware Environment on page 39](#)
- [Preparing to Integrate Firefly Host with the VMware Environment on page 43](#)
- [Understanding Firefly Host Environment Time Synchronization on page 44](#)
- [Firefly Host VMsafe Firewall + Monitoring and VMsafe Monitoring Modes on page 44](#)

Firefly Host Prerequisites and Resource Requirements for the VMware Environment

This topic covers how to prepare to install the Firefly Host product for integration and deployment in the VMware vSphere environment. It covers prerequisites and identifies the resources required to import the Firefly Host into the VMware environment, install the product, and run it.

This topic includes the following sections:

- [Overall Resource and Access Requirements on page 39](#)
- [Virtual Appliance System Requirements on page 40](#)
- [Firefly Host VMware vSwitch Requirements on page 41](#)
- [VMware Port Group Requirements on page 42](#)
- [Virtualized NIC Requirements on page 43](#)

Overall Resource and Access Requirements

Ensure that the following resources are available:

- One or more vSphere ESX/ESXi 4.x hosts. Beginning with Release 5.0r2, Firefly Host is enhanced to provide support for vSphere 5.1.

We recommend that you use more than one host for your deployment.



NOTE: vSphere 5.1 supports only ESXi hosts.

You use the VMware vSphere Client software to integrate the Firefly Host with the VMware infrastructure.

- A VMware Virtual Center (vCenter) server, version 4.x. vGW Series 5.0r2 and later releases also support vCenter 5.0.

The vCenter VMware management server oversees the virtualization data center. The vCenter can be a physical server or a VM running on an MS Windows server.

The vCenter server automatically imports Firefly Host components, and it adapts security as necessary when changes are made to the virtualized environment.

- Network connectivity.

The Firefly Host Dashboard must be accessible through HTTPS to allow access to the VMware Virtual Infrastructure API. Access to the VMware Virtual Infrastructure API is also required for autodiscovery of VM resources.

If you have access to the VMware Virtual Infrastructure API, you can connect a Web browser to the vCenter host (<https://vCenter-IP-address>).

- Domain Name System (DNS) and Network Time Protocol (NTP) services for some components.

The Firefly Host VM requires NTP access to the center.

- One of the following supported Web browsers is required:
 - Microsoft Internet Explorer 7, 8, or 9
 - Mozilla Firefox 3 or later



NOTE: Localized (non-English) versions of browsers, such as the Japanese version of IE7, are not fully supported. However, most character sets including Japanese should display properly.

Virtual Appliance System Requirements

You can configure a network attached storage (NAS) device or a local datastore to use for both the Firefly Host Dashboard and the Firefly Host VM. However, we recommend the following:

- Store the Firefly Host Dashboard on a NAS device so that it can be VMotioned.

You can allow the Firefly Host Dashboard to be migrated between hosts because it is not tied to a specific ESX/ESXi host.

Because the Firefly Host Dashboard can be sensitive to a slow NAS device, you should monitor it closely.

- Store each Firefly Host VM on a local datastore on the ESX/ESXi host where it is installed.

A Firefly Host VM is installed on and always remains associated with a single ESX/ESXi host. The Firefly Host VM is configured not to be migrated through VMotion because it is specific to its host. If the host becomes unavailable, its Firefly Host VM is not used for another host. It is applicable only to the host to which it was initially deployed. Allowing a Firefly Host VM to migrate can cause problems in the virtualized environment.

If you must, you can place the Firefly Host VMs on a NAS device. In this case, ensure that the Firefly Host VMs are not VMotioned away from their designated hosts.



NOTE: Do not use a read-only datastore.

- The virtual appliances assume the following memory and require the following disk space:
 - [Table 6 on page 41](#) lists the Firefly Host Dashboard specifications.

Table 6: Firefly Host Dashboard Specifications

Component	Specification
Memory	For Firefly Host Release 6.0, you can configure up to 7 GB. For earlier versions, use 3 GB.
Disk space	11GB

- [Table 7 on page 41](#) lists the Firefly Host VM specifications.

Table 7: Firefly Host VM Specifications

Component	Specification
Memory	1GB WARNING: Do not manipulate the memory size of the Firefly Host VM. It must remain 1 GB.
Disk space	1.5 GB
vCPU	1

Firefly Host VMware vSwitch Requirements

VMware lets you create abstracted network devices called virtual switches (vSwitches). A vSwitch routes traffic internally between virtual machines, and it links to external networks. A vSwitch works somewhat like a physical Ethernet switch. It detects which

virtual machines are logically connected to its virtual ports to enable it to forward traffic to the correct virtual machines.

A vSwitch can be connected to physical switches using physical Ethernet adapters, also referred to as uplink adapters, to join virtual networks with physical networks. This process is similar to connecting physical switches to create a larger network. Even though a vSwitch works like a physical switch, it does not have the advanced functionality of a physical switch.

For the Firefly Host:

- You can map a vSwitch to one or more physical NICs on the ESX/ESXi host server, although this is not a requirement.
- You can configure features such as QoS traffic shaping on a vSwitch.

Firefly Host interoperates with the following types of switches:

- Standard VMware Virtual Switch
- VMware Distributed Virtual Switch (DVS)
- Cisco Nexus 1000V device



WARNING: Firefly Host creates a vmservice-switch for its own use. Do not make changes to its configuration or in anyway affect it.

VMware Port Group Requirements

In the VMware virtualized environment, port groups are used to aggregate multiple ports under a common configuration. They serve as an anchor point for virtual machines that connect to labeled networks. Each port group is identified by a network label. If port groups are configured, they are often mapped to VLANs, although this is not necessarily the case.

An administrator assigns to a port group a virtual network interface card (NIC) that connects a VM with a vSwitch.

There are two types of port groups:

- Virtual machine port groups. We recommend that you create a port group designated for a few test VMs to be secured.
- VM kernel port groups. This type of port group is used for storage for VMotion and ESX/ESXi host management.

We recommend that you create a port group designated for communication between the Firefly Host Dashboard and the management interfaces on each of the Firefly Host VMs. For example, you might call this port group Juniper Networks Firefly Host Management. You can associate this port group with a VLAN, but it must not filter TCP 443 or TCP 8443. There must be IP address space available for the Firefly Host Dashboard interface and for each of the Firefly Host VMs.

You can use the preexisting VMware Management port group for this purpose.



WARNING: Firefly Host creates two port groups that it uses to connect the VMsafe network to the Firefly Host Module for communication. Do not change the configuration of these port groups in any way. They are for internal use only. The monitor port group is used when you activate console monitoring. It is a promiscuous port group that Firefly Host uses to view traffic into the service console for Network module tracking and IDS. You might notice that these port groups are created when you install Firefly Host:

```
Altor_TVAm_Monitor_
vmervice-altor
vmervice-vmknic-pg
```

Virtualized NIC Requirements

Consider the following details when configuring vNICs:

- Do not change the Firefly Host VM and the Firefly Host Dashboard vNICs default configuration. By default, vNICs are set to connect when they are powered on.
- VMs can use any type of vNIC supported by VMware. For example, their administrators might want to use VMXNET3 for improved performance. Additionally, the Firefly Host supports multiple vNICs for a VM. You can secure these vNICs with different policies using the Policy per vNIC feature. For details, see *Configuring the Firefly Host Policy per vNIC Feature*.

Related Documentation

- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 48](#)
- [Understanding Firefly Host on page 3](#)
- [Integrating the Firefly Host with VMware Using the Settings Module](#)
- [Installing Firefly Host VMs on ESX/ESXi Hosts](#)

Preparing to Integrate Firefly Host with the VMware Environment

Before you import and install Firefly Host with the VMware environment, take the following precautions:

- Ensure that the virtual machines (VMs) in your environment can communicate with one another. You can use the ping command for this purpose.
- Ensure that you can access the ESX/ESXi hosts using SSH.
- Verify that Domain Name System (DNS) and Network Time Protocol (NTP) services are functioning properly on the network.
- Ensure that there is HTTP access to the datastore. By default, vCenter allows this access. However, if you have hardened your configuration by adding false to your

vpxd.cfg file, Firefly Host will not be able to automatically deploy the Firefly Host Module.

- Related Documentation**
- [Understanding the VMware Infrastructure and Firefly Host on page 7](#)
 - [Understanding Firefly Host on page 3](#)
 - [Firefly Host Prerequisites and Resource Requirements for the VMware Environment on page 39](#)

Understanding Firefly Host Environment Time Synchronization

Firefly Host uses NTP to synchronize all times in the environment to ensure that all security policies, logs, and other time-based data, are properly marked. Large time gaps resulting from improperly configured systems can cause unexpected results and make it difficult to troubleshoot the environment.



WARNING: Do not edit the time settings, including the time zone, for a Firefly Host Dashboard directly. The Firefly Host VMs obtain their time setting from the Firefly Host Dashboard. Inappropriate changes made to the Firefly Host Dashboard can adversely affect all Firefly Host VMs.

Take care in configuring NTP when you install Firefly Host. Ensure that the internal NTP server is up and functioning properly, and that outbound Internet access to an Internet time server is available.

See *Configuring Firefly Host Time Settings*.

- Related Documentation**
- [Understanding Firefly Host on page 3](#)
 - [Understanding the Firefly Host Dashboard on page 11](#)
 - [Installing an Additional Firefly Host Dashboard and Configuring the Primary Firefly Host Dashboard to Use It for High Availability](#)
 - [Installing a Secondary Firefly Host VM for High Availability](#)

Firefly Host VMsafe Firewall + Monitoring and VMsafe Monitoring Modes

Firefly Host supports two modes that allow you to secure and observe virtual machines (VMs) and traffic:

- VMsafe Firewall + Monitoring mode allows you to secure specific VMs or entire port groups. It provides visibility into all traffic that transits each protected VM.
- VMsafe Monitoring mode allows you to fully monitor VMs without securing them. It guarantees that no packets are blocked because of an incorrectly configured security policy. When monitoring mode is enabled, security policies are not loaded into the Firefly Host hypervisor module.

When this option is selected and you create a group for which you do not select the Policy Group option, the group is automatically placed in the Monitoring Groups section of the VM tree. (To create a group, use the Settings module Security Settings > Groups page.) For details on creating groups, see *Understanding Firefly Host Groups*.

To use VMsafe Monitoring mode:

1. First enable it. On the Settings module Firefly Host Application Settings > Install Settings page, select the **Enable Monitoring-only option for VMsafe** checkbox.
2. If VMsafe Monitoring mode is enabled, when you use the Settings module Firefly Host Application Settings > Installation page to install a Firefly Host VM, you can choose either VMsafe Firewall+Monitoring or VMsafe Monitoring for the installation.

To view monitoring groups, use the Settings module > Security Settings > Groups page, and select **Monitor Groups**. The table shows all configured monitoring groups.

When Firefly Host installs a Firefly Host VM on an ESX/ESXi host in either VMsafe Firewall + Monitoring mode or VMsafe Monitoring mode, it uses the VMware VMsafe networking APIs to build the security engine as a Firefly Host module in the hypervisor of the host.

This installation allows for full protocol inspection of every VM.

**Related
Documentation**

- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host VM on page 24](#)
- [Installing Firefly Host VMs on ESX/ESXi Hosts](#)
- [Understanding the Firefly Host Dashboard on page 11](#)

CHAPTER 6

OVA and Firefly Host Deployment

- [Understanding the Open Virtualization Format OVA Template Method on page 47](#)
- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 48](#)
- [Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware on page 56](#)
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 58](#)

Understanding the Open Virtualization Format OVA Template Method

Firefly Host leverages the Open Virtualization Format (OVF) standard for packaging and delivering virtual machines (VMs). The OVF supports industry-standard content verification and integrity checking, and it provides a basic scheme for managing software licensing. As described by the standard, OVF defines an "open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines." The standard also supports the OVA template method of packaging and distributing software in a single archive. You use the vSphere 4.x client to load the OVA file.

You can use OVA to deploy the Firefly Host VMs in the following ways:

- In a single bundled OVA package, also referred to as a Combo Package that contains the Firefly Host Dashboard and the Firefly Host VM template.

Firefly Host uses OVA to deliver a single file containing both Firefly Host components.

- In nonbundled OVA files to separately deploy the Firefly Host Dashboard and the Firefly Host VM template.

The OVA Combo Package installs a vApp, and VMware will not install a vApp on a cluster for which the Dynamic Resource Scheduler (DRS) is not enabled. You can take the nonbundled approach in this case.

The nonbundled OVA approach is also useful for installing the most current Firefly Host VM, after the initial installation, to ensure that the latest version is used for automatic Firefly Host VM instantiation on ESX/ESXi hosts.

You can also use it to create a secondary Firefly Host Dashboard for high availability. For details, see *Installing an Additional Firefly Host Dashboard and Configuring the Primary Firefly Host Dashboard to Use It for High Availability*.

Related Documentation

- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 58](#)
- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 48](#)
- [Preparing to Integrate Firefly Host with the VMware Environment on page 43](#)
- [Understanding the VMware Infrastructure and Firefly Host on page 7](#)
- [Understanding Firefly Host on page 3](#)

Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure

This topic explains how to integrate the Firefly Host appliances—the Firefly Host Dashboard and the Firefly Host VM template—with the VMware virtualized infrastructure.

For information on “Firefly Host Prerequisites and Resource Requirements for the VMware Environment” on page 39 see “Firefly Host Prerequisites and Resource Requirements for the VMware Environment” on page 39.

This topic includes the following sections:

- [Requirements on page 48](#)
- [Overview on page 48](#)
- [Downloading the Firefly Host OVA Combo Package on page 49](#)
- [Integrating the Firefly Host with the VMware Infrastructure on page 49](#)

Requirements

For information, see “Firefly Host Prerequisites and Resource Requirements for the VMware Environment” on page 39.

Overview

The bundled OVA template allows you to deploy both the Firefly Host Dashboard and the Firefly Host VM appliances in a single OVA archive file. In this case, OVA creates a single vApp and inserts the two Firefly Host appliances into it.

You can delete the vApp after the deployment and integration process is complete. It is used only to convey the Firefly Host VMs. However, take care not to delete it before then.

In the single Combo Package file, the OVA template deploys:

- The Firefly Host Dashboard
- The Firefly Host VM

You must manually convert the Firefly Host VM to a template after you integrate the Firefly Host with the VMware infrastructure. Firefly Host uses the resulting template to instantiate a Firefly Host VM on each ESX/ESXi host when you secure that host.



NOTE: The OVA Combo Package installs a vApp, and VMware will not install a vApp on a cluster for which DRS is not enabled. In this case, you must use the nonbundled OVA method to deploy each component separately.

- For details, see “Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware” on page 56.
- For details, see “Using the OVA Single File Method to Integrate the Firefly Host VM with VMware” on page 58.

The Firefly Host software packages are available at:

<http://www.juniper.net/support/downloads/>.

Downloading the Firefly Host OVA Combo Package

Step-by-Step Procedure To download the Juniper Networks OVA archive file that contains both the Firefly Host Dashboard and the Firefly Host VM:

1. Navigate to the Juniper Networks Support page.
2. Select **Software Downloads** from the Support box in the left column.
3. Select **Firefly Host (Altor)** in the Security pane.
4. Select the **Software** tab.
5. Click **Firefly Host 6.0 Combo Package**, and log in to the site to download the file.

Integrating the Firefly Host with the VMware Infrastructure

Step-by-Step Procedure To deploy the Firefly Host appliances—the Firefly Host Dashboard and the Firefly Host VM—and integrate them with the VMware infrastructure:

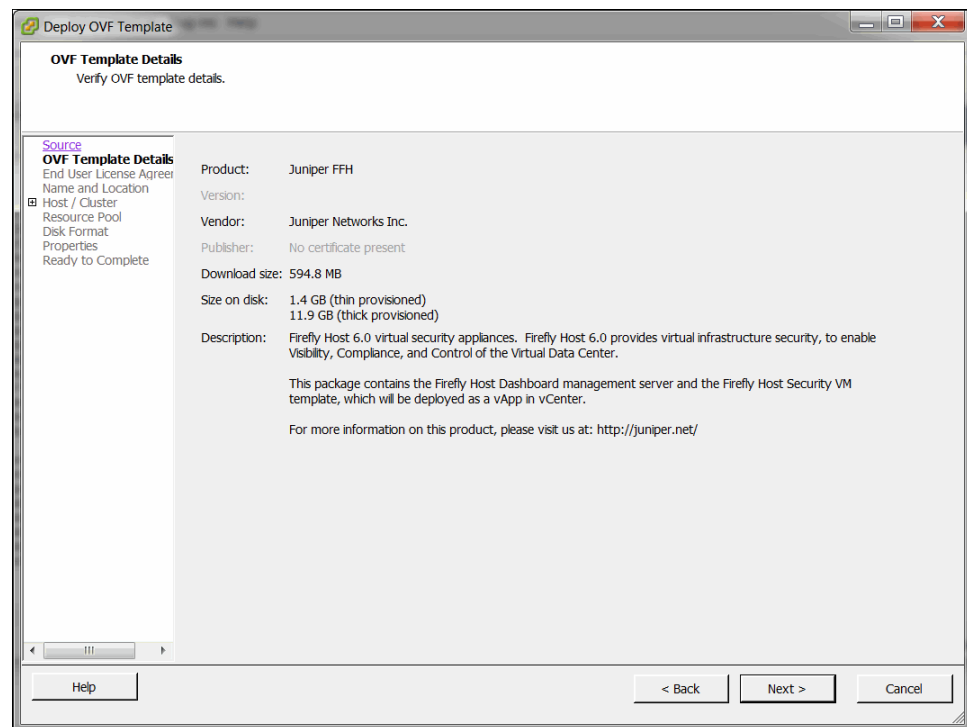
1. Using the vSphere client, load the bundled OVA file. Select **Deploy OVF Template** from the File menu.
2. Enter the download filename or its URL in the Deploy from file or URL box—for example, enter: `c:\temp\Firefly_Host_Combo_6.0_#-#-#_#-#-#.ova`—and click **Next**.

You use the OVF template method to deploy the OVA file. After you specify the name of the OVA file and its location, the Appliance Wizard displays the OVA template details dialog box.

3. Verify the contents of the OVA package, and click **Next**.

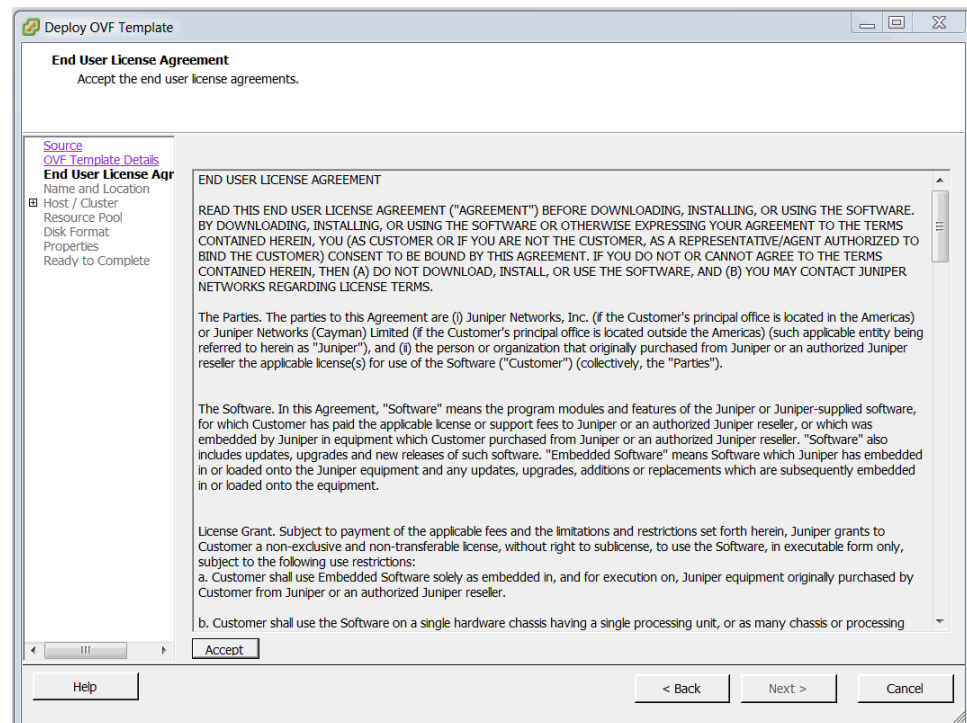
Before the wizard unbundles the OVA package, verify that it contains the Firefly Host appliances. The OVA template summary also specifies the disk space requirements for thick and thin provisioning. See [Figure 26 on page 50](#).

Figure 26: OVA Template Details Page



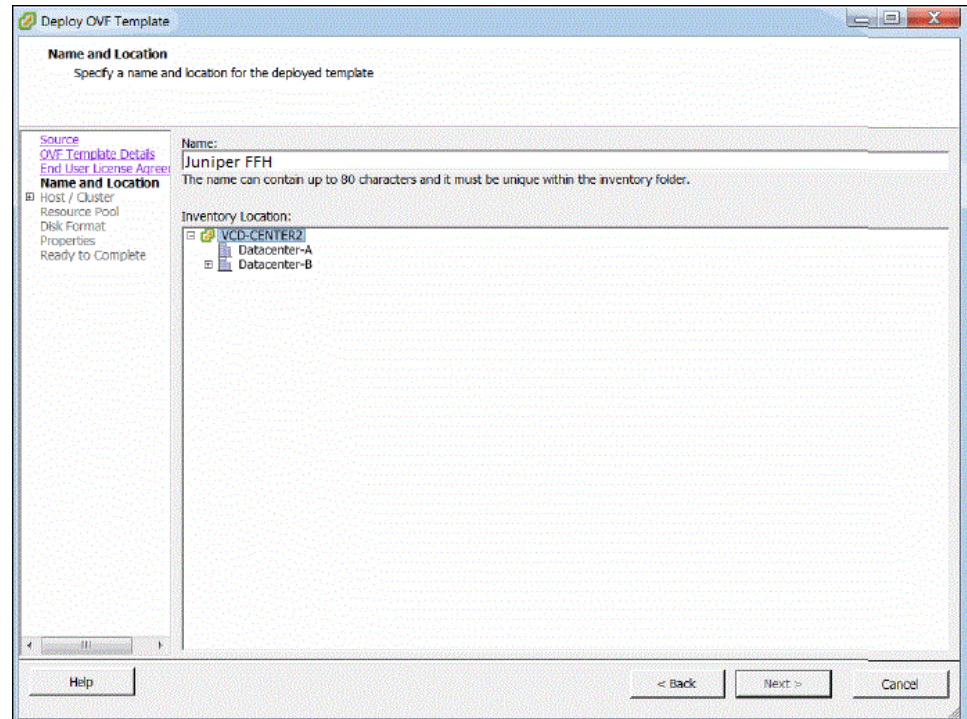
4. Accept the Firefly Host license agreement, and click **Next**. See Figure 27 on page 50.

Figure 27: OVA File Deployment License Agreement



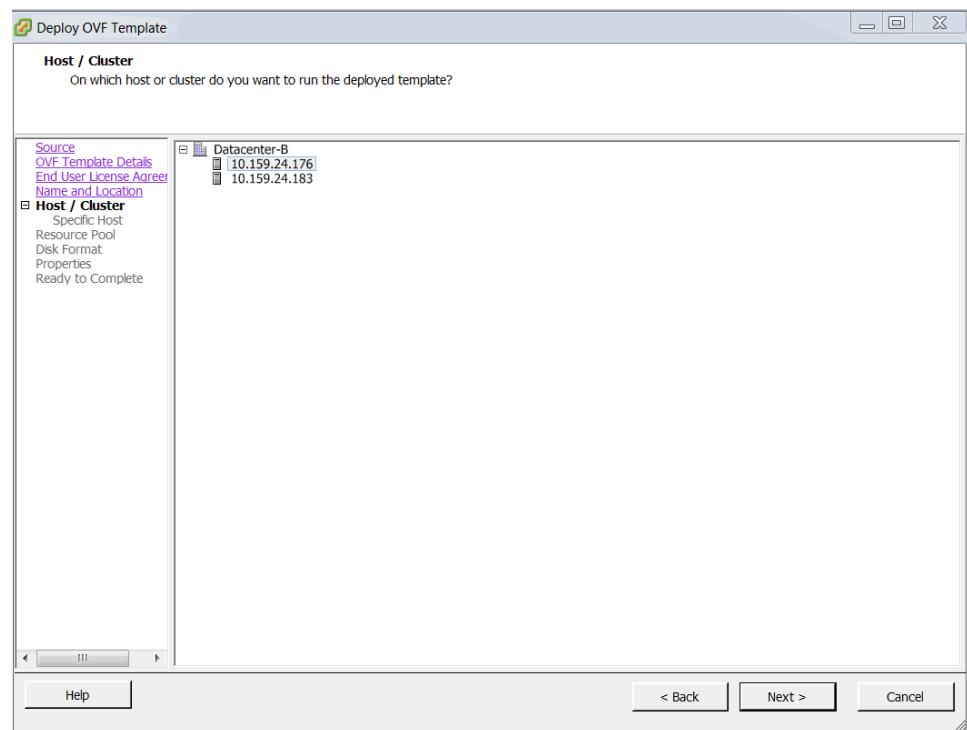
5. Specify a name for the vApp that will be created and a storage location. See [Figure 28 on page 51](#).

Figure 28: Naming the vApp



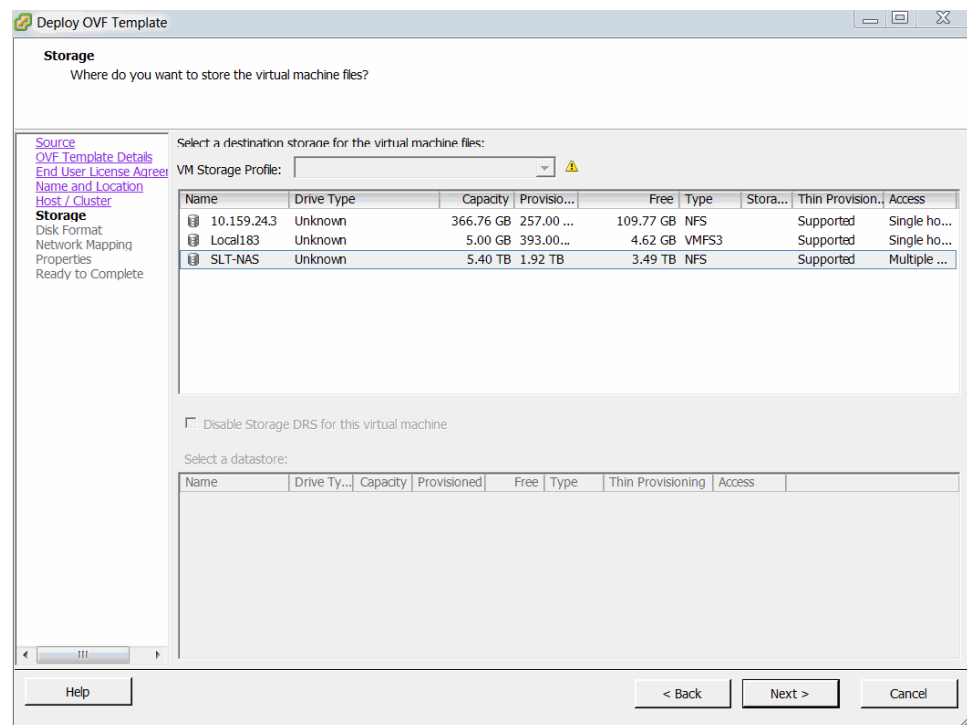
6. Specify the host or host/cluster on which to run the deployed template. We recommend that you use a network storage device (NAS) so that it can be migrated through VMotion for space optimization. See [Figure 29 on page 52](#).

Figure 29: Specifying the Host and Cluster



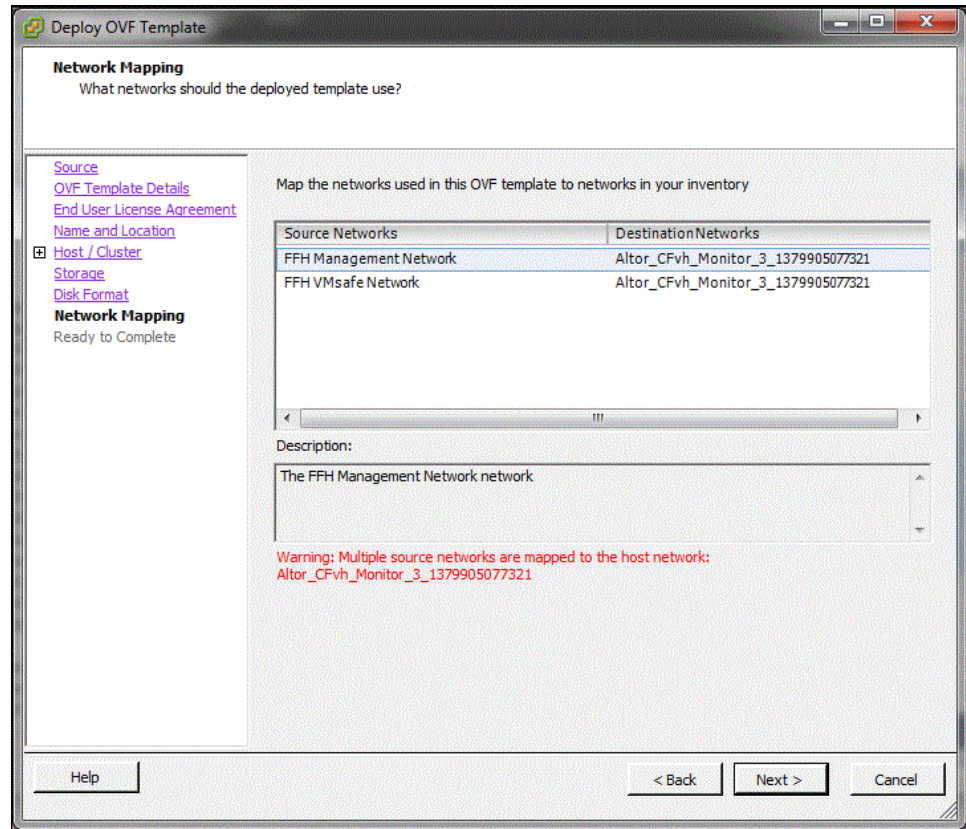
7. Select the datastore. Do not use a read-only datastore. [Figure 30 on page 52.](#)

Figure 30: Selecting the Storage



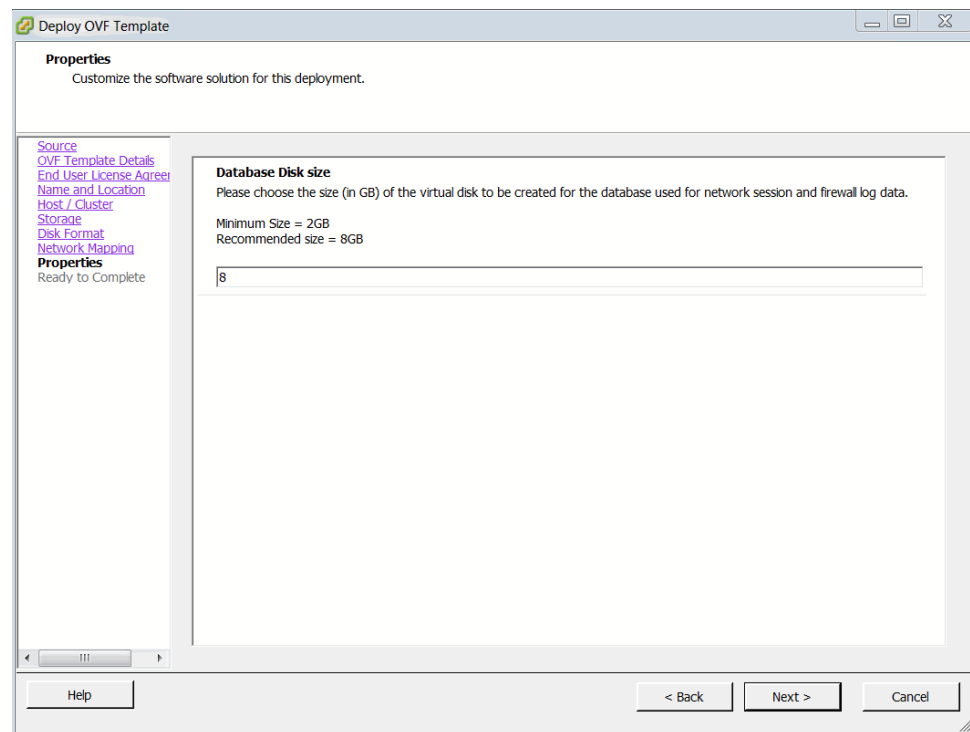
8. Select the disk format. Accept the thick provisioned format default. Thick provisioning preallocates all required space for the product.
9. Map the networks. Set the Firefly Host management network to a destination network that is accessible to vCenter and the Firefly Host Dashboard. See [Figure 31 on page 53](#).

Figure 31: Mapping the Firefly Host Management Networks



10. Specify the size of the database to use for storing Firefly Host files.
The database stores network connection records and firewall logs.
See [Figure 32 on page 54](#).

Figure 32: Specifying the Database Disk Size

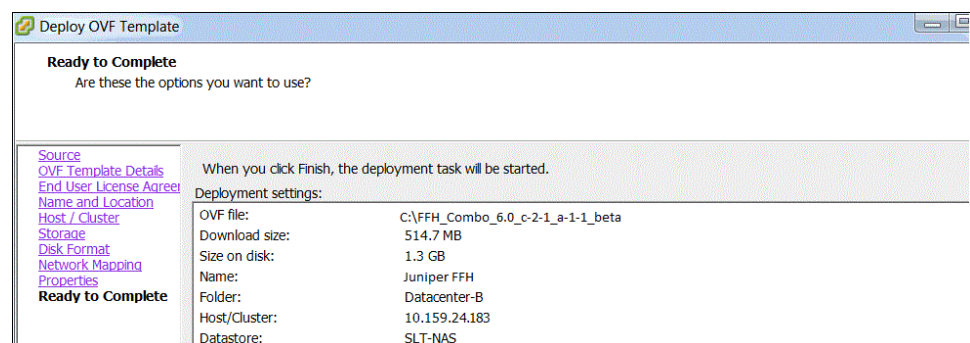


The default disk size is 8.0 GB. In a typical environment that includes 5 to 10 ESX/ESXi hosts, a database of this size can accommodate data accumulated over several months. However, for your environment you might want to deploy a database that is larger than 8.0 GB.

You can increase the database size later if you find that the current space is not adequate. Although there is no hard-coded limit, we recommend restricting the size to less than 75 GB.

11. Verify that the configuration is correct, and click **Finish** to complete the deployment. See [Figure 33 on page 54](#).

Figure 33: Verifying That the Configuration Is Correct

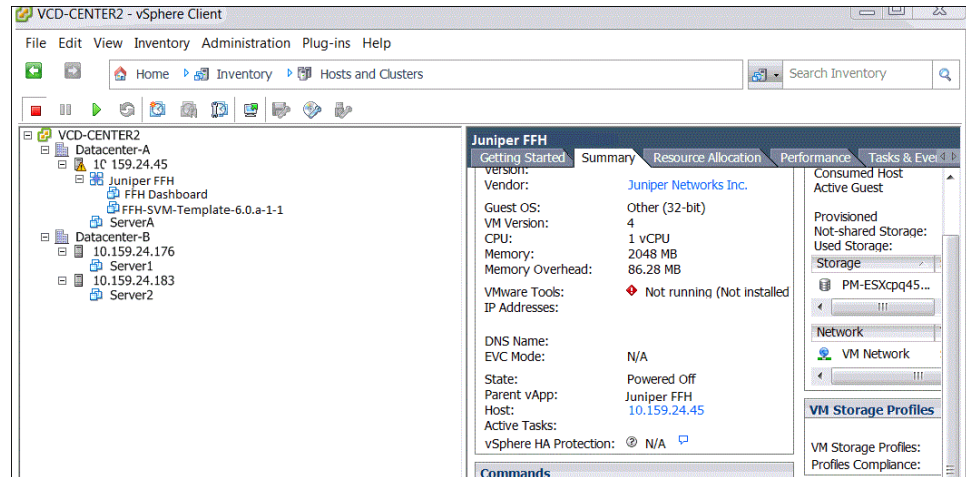


The Virtual Appliance Wizard downloads the files and inserts the Firefly Host VMs as a single virtual appliance (vApp) into the VMware infrastructure.

When the OVA import is completed, the vCenter includes the vApp containing both the Firefly Host Dashboard and the Firefly Host VM template components.

12. Expand the appliance called Juniper Firefly Host 6.0 to display the Firefly Host Dashboard and the Firefly Host VM. See [Figure 34 on page 55](#).

Figure 34: Displaying the Firefly Host Appliance Components



Move the two Firefly Host VMs out from the vAPP. Afterward you can delete the vApp if you choose to, but it is not necessary.



NOTE: Firefly Host uses the VMware vApp deployment feature as a vehicle to deliver multiple VMs in the same OVA file. The vApp structure is redundant after it is used for deployment, and therefore you can delete it. However, do not delete the vApp without first having moved the Firefly Host VMs out from it. If you do, the newly created Firefly Host VMs would be deleted when you delete the vApp.

After you remove the Firefly Host VMs from the vApp:

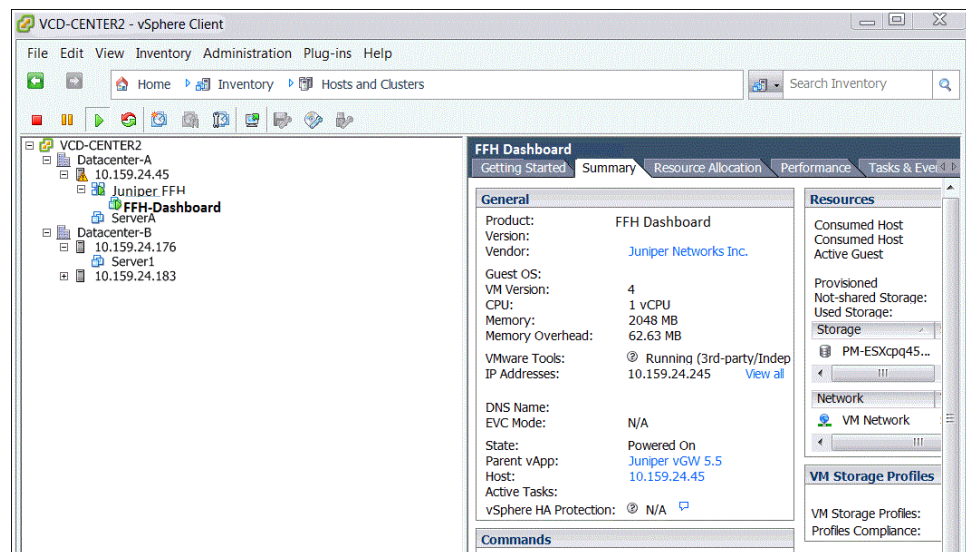
- a. Convert the Firefly Host-Firefly Host VM-Template VM to a template that the Firefly Host Dashboard and installer can use to instantiate a Firefly Host VM on each ESX/ESXi host to be secured.

Right-click the template, select **Template**, and select **Convert to Template**.

- b. Right-click the Firefly Host Dashboard and power it on. [Figure 35 on page 56](#) shows the vCenter summary information for the Firefly Host Dashboard.

[Figure 35 on page 56](#) shows the vCenter summary information for the Firefly Host Dashboard.

Figure 35: Firefly Host Dashboard Summary Tab in vCenter



Related Documentation

- [Firefly Host Prerequisites and Resource Requirements for the VMware Environment on page 39](#)
- [Understanding Firefly Host on page 3](#)
- [Understanding the VMware Infrastructure and Firefly Host on page 7](#)
- [Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware on page 56](#)
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 58](#)
- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host VM on page 24](#)

Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware

This topic explains how to download and deploy a single OVA file containing the Firefly Host Dashboard.

To download an OVA file containing the Firefly Host Dashboard appliance and deploy it:

1. Download the Juniper Networks Firefly Host OVA file.
 - a. Navigate to the Juniper Networks Support page.
 - b. Select **Software Downloads** from the Support box in the left column.
 - c. Select **Firefly Host (Altor)** in the Security pane.

- d. Select the **Software** tab.
- e. Click **DashboardFirefly Host 6.0**, and log in to the site to download the file.
2. Load the OVA file for the Firefly Host Dashboard using the vSphere 4.x client (File > Deploy OVF Template), and enter the name of the OVA download file in the Deploy from file or URL box.

For example, enter: `c:\temp\DashboardFireflyHost.ova`.

3. Follow the Virtual Appliance Wizard process, and select the appropriate options for your environment.
4. Click **Finish** to download the files and integrate the Firefly Host Dashboard with the VMware infrastructure.

After the Firefly Host Dashboard import process is completed, you must add a virtual hard disk for it.



NOTE: This step is not required for the bundled approach because it is done automatically.

The default disk size is 8.0 GB. In a typical environment that includes 5 to 10 ESX/ESXi hosts, a database of this size can accommodate data accumulated over several months.

For your environment you might want to deploy a database larger than 8.0 GB. Note that you can increase the database size later if you find that the current space is not adequate. The disk should not be thin-provisioned.

5. Add a disk to be used as the datastore:
 - a. Select **Firefly Host Dashboard**.
 - b. Select the **Summary** tab, and click **Edit Settings > Add a Hard Disk virtual device**.

This disk is used for the database that stores network connection records and firewall logs. Select a NAS device so that VMotion can be used to migrate the datastore.

6. Power on the Firefly Host Dashboard.

Related Documentation

- [Firefly Host Prerequisites and Resource Requirements for the VMware Environment on page 39](#)
- [Understanding Firefly Host on page 3](#)
- [Understanding the VMware Infrastructure and Firefly Host on page 7](#)
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 58](#)
- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host VM on page 24](#)

Using the OVA Single File Method to Integrate the Firefly Host VM with VMware

To download a nonbundled OVA file containing the Firefly Host VM and deploy it:

1. Load the OVA file for the Firefly Host VM using the VMware vSphere Client (File > Deploy OVF Template), and insert the template name Firefly Host-Firefly Host VM-Template in the Deploy from file or URL box. For example, enter **c:\temp\Firefly Host-Firefly Host VM-Template.ova**.

2. Select the appropriate options for your environment in each of the steps presented by the Virtual Appliance Wizard.

Configure the host/cluster, resource pool, and so on, that is appropriate for your environment.

When you are asked for network mapping information, accept the default settings. Firefly Host automatically configures these settings later.

3. When the Virtual Appliance Wizard completes, right-click the resulting VM and select **Template > Convert to Template**.

You can use the resulting template to automate installation of Firefly Host VMs on ESX/ESXi hosts to secure parts of your virtual network. The Firefly Host Dashboard and installer require the template to instantiate the Firefly Host VM on hosts to be secured.

Related Documentation

- [Firefly Host Prerequisites and Resource Requirements for the VMware Environment on page 39](#)
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 58.](#)
- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 48](#)
- [Preparing to Integrate Firefly Host with the VMware Environment on page 43](#)

PART 3

Firefly Host Setup

- [Firefly Host Dashboard Setup Process on page 61](#)

CHAPTER 7

Firefly Host Dashboard Setup Process

- [Setting Up Firefly Host on page 61](#)

Setting Up Firefly Host

After you download and integrate Firefly Host with the VMware environment and power on the Firefly Host Dashboard, you can configure its basic system parameters. This topic explains how to connect to the Firefly Host Dashboard to configure basic settings. It describes how to use the Firefly Host wizard to configure those settings initially.

This topic includes the following sections:

- [Determining the Firefly Host Dashboard's Default IP Address on page 61](#)
- [Changing or Setting the IP Address for the Firefly Host Dashboard on page 63](#)
- [Connecting to the Firefly Host Dashboard and Configuring Basic Settings on page 64](#)

Determining the Firefly Host Dashboard's Default IP Address

To access the Firefly Host Dashboard, you enter its IP address in a supported Web browser.

When you powered on the Firefly Host Dashboard during Firefly Host integration with VMware, which is described in ["Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure" on page 48](#), it acquired an IP address that you can view on the vCenter Summary page.

By default, the Firefly Host Dashboard is configured to use IPv4 DHCP to acquire its address. If problems occur and it cannot obtain an IP address in this manner, it tries other methods. In order, these are the three methods that the Firefly Host Dashboard uses in an attempt to obtain an IP address:

- IPv4 DHCP
- IPv6 autoconfiguration

With stateless IPv6 autoconfiguration, the Firefly Host Dashboard acquires its IPv6 address automatically without the intervention of a DHCP server.

- IPv6 DHCPv6



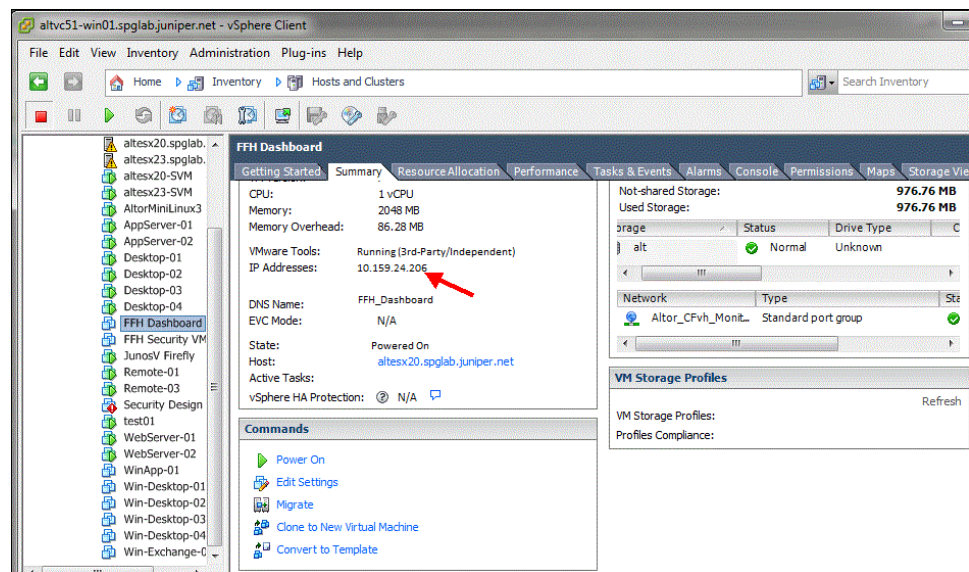
NOTE: If DHCP is not available on the Firefly Host Dashboard network, you can log into the console using admin for both the username and the password. Type config network at the command prompt and proceed through the options to assign an IP address. After an IP address is set—whether DHCP or static, you can access the Firefly Host Dashboard through a Web browser.

To view the IP address bound to the Firefly Host Dashboard:

1. Launch the VMware vSphere Client, and select the Firefly Host Dashboard icon on the left navigation pane.
2. Select the **Summary** tab.

The IP address that was acquired appears in the IP Addresses: field. See [Figure 36 on page 62](#).

Figure 36: Viewing the Firefly Host Dashboard IP Address in VMware



After you have obtained the IP address, follow the instructions in [“Connecting to the Firefly Host Dashboard and Configuring Basic Settings” on page 64](#) to configure the basic settings.

Changing or Setting the IP Address for the Firefly Host Dashboard

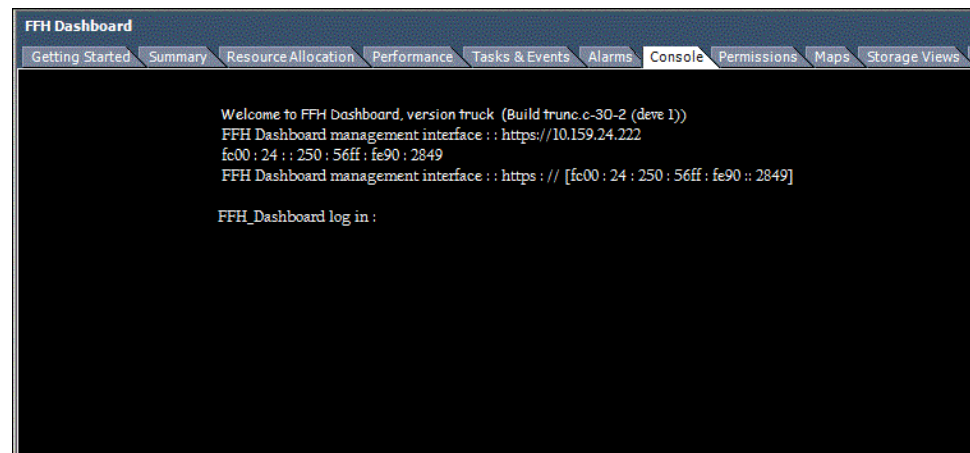
You can use the Firefly Host command-line interface (CLI) to set the IP address for the Firefly Host Dashboard.

To use the Firefly Host CLI from the vCenter console:

1. Launch the VMware vSphere Client.
2. Right-click the Firefly Host Dashboard icon on the left navigation panel to display a list of options.
3. Select the third option on the list, **Open Console**. Alternatively you can select the **Console** tab, as shown in [Figure 37 on page 63](#).

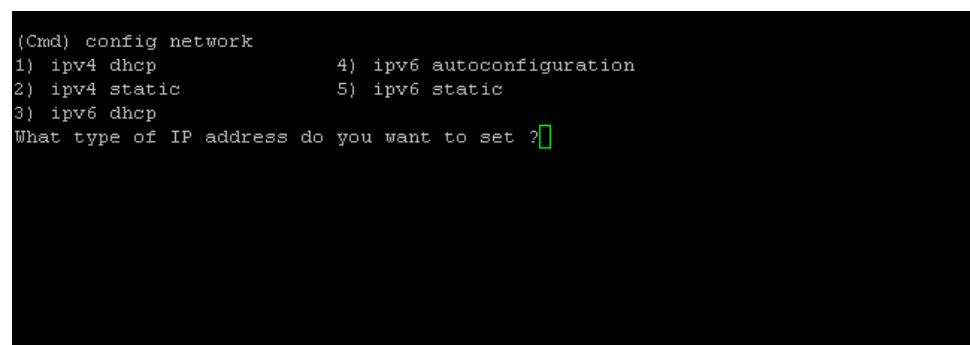
The console window appears.

Figure 37: Firefly Host Dashboard IP Addresses on the Firefly Host CLI Console



4. At the CLI prompt enter **config network**. Enter **admin** for both the username and password. In this mode you can configure the IP address for the Firefly Host Dashboard. You can specify an IP address for either IP protocol family. See [Figure 38 on page 63](#).

Figure 38: Configuring an IP Address for the Firefly Host Dashboard



5. In response to the prompt **What type of IP address do you want to set?** enter the number preceding the type of IP address that you want to be assigned to the Firefly Host Dashboard and how it is to be acquired.

For example, the administrator might enter **4** for **4) ipv6 autoconfiguration**.

6. The Firefly Host CLI gives you the opportunity to cancel by presenting the prompt **Are you sure?**. If you enter **y** for **yes**, Firefly Host shuts down the interface and brings it back up with the new IP address.

Connecting to the Firefly Host Dashboard and Configuring Basic Settings

This section explains how to set up the Firefly Host Dashboard initially.

1. Using a supported Web browser, connect to the Firefly Host Dashboard management interface through HTTPS. Enter the IP address of the Firefly Host Dashboard in the Web browser.

This is the IP address that was assigned when you powered on the Firefly Host Dashboard.

Firefly Host supports the following Web browsers:

- Microsoft Internet Explorer 7, 8, and 9
- Mozilla Firefox 3 or later

2. Enter **admin** for both the username and password. See [Figure 39 on page 64](#).

Figure 39: Logging In to the Firefly Host Dashboard



Firefly Host Dashboard

JUNIPER NETWORKS

Username: admin

Password: admin

Submit

Copyright © 2013 Juniper Networks, Inc. | [All rights reserved](#) | [Legal Notices](#) | [Privacy](#)

3. Read the information message, and review the process overview shown in the Wizard Progress pane. See [Figure 40 on page 65](#).

Figure 40: Firefly Host Installation Wizard Overview

Firefly Host Installation Wizard

Wizard Progress

1. Introduction
2. Change Default Password
3. Network Setup
4. Time Configuration
5. Product License
6. Virtual Center Settings
7. Reports
8. Firefly Host VM Template Selection
9. Summary

Introduction

This installation wizard will assist you in the initial configuration of your Firefly Host management server. Some information that will be necessary to complete this process includes:

- DHCP or Static IP Address.
If using static addressing, an available IP address, netmask, default route, and DNS server address will be needed.
- Network Time Protocol (NTP) Server address.
- VMware vCenter login credentials.
- A Firefly Host license, either evaluation or full license, if available.

[Prev Step](#) [Next Step](#)

4. Change the default Firefly Host global administrator account password—admin—that you used to log in.

You must change the default password. See [Figure 41 on page 65](#). Store the new password in a secure location. It is difficult to recover a lost or forgotten global administrator account password. If you wish, you can change the password that you specify here later, but to do so you must enter your current password, which would be the one that you configured here.



TIP: You can integrate administration accounts with the Firefly Host Dashboard after the installation is completed. For information on how to do that later, see *Adding New Firefly Host Administrator Definitions, Permissions, and Authentication Using the Settings Module*.

Figure 41: Changing the Default Password

Firefly Host Installation Wizard

Wizard Progress

1. Introduction
2. Change Default Password
3. Network Setup
4. Time Configuration
5. Product License
6. Virtual Center Settings
7. Reports
8. Firefly Host VM Template Selection
9. Summary

Change Default Password

Please select a new password for the default global administrator account. The user-name for this account is "admin". The "admin" account can also be used to login to the console of the virtual machine for advanced configuration.

Current Password:

New Password:

Confirm New Password:

[Prev Step](#) [Next Step](#)

5. Configure networking parameters for the Firefly Host Dashboard.



NOTE: If you changed the IP address, you must log in to the system again. Changes to the IP address take effect immediately.

Set the correct destination network for the Firefly Host Dashboard and leave the VMsafe Network unchanged. At this point you can configure other network information for the Firefly Host Dashboard, such as whether to use dual stack for it and how it obtains its management interface addresses.

A dual-stack device can connect to an IPv4-only device or an IPv6-only device, or it can connect to another device that implements dual stack.

For its management interface addressing mode, either accept the default dual stack values of DHCP for IPv4 and DHCPv6 for IPv6 or change the values by selecting:

- IPv4
 - DHCP (Default): To obtain an IPv4 address, by default the Firefly Host Dashboard is configured to use DHCP. You do not need to specify additional information.
 - Static IP. If you select **Static IP**, you must specify a static IPv4 address and its network mask routing prefix, and the default gateway to assign to the Firefly Host Dashboard.
- IPv6
 - DHCPv6 (Default): To obtain an IPv6 address, by default the Firefly Host Dashboard is configured to use DHCPv6. You do not need to specify additional information.
 - Autoconfiguration. If you select **Autoconfiguration**, stateless address autoconfiguration is used to obtain the IPv6 address. It allows network devices attached to an IPv6 network to automatically acquire IP addresses and connect to the Internet without intermediate interaction with a DHCPv6 server.
 - Static IP. If you select **Static IP**, you must specify a static IPv6 address, including the IPv6 address prefix (the initial bits of the address that denote the network address, akin to a netmask), and the default gateway to use for it.



NOTE: By default, a dual stack Firefly Host Dashboard communicates with a Firefly Host VM using the IPv4 protocol. However, you can use the Firefly Host 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 Firefly Host Dashboard is configured for dual stack and one or more Firefly Host VMs is also configured for dual stack. In all other cases, the protocol used is the one that is common to both the Firefly Host Dashboard and the Firefly Host VM, and this parameter is irrelevant.

If you do not want the Firefly Host Dashboard to be configured for dual stack which is its default configuration, you can change the configuration in the following way:

- To use only IPv4 for Firefly Host Dashboard management communication with its Firefly Host VMs, disable IPv6. On the displayed list for the IPv6: box, select **Disabled**.
- To use only IPv6 for Firefly Host Dashboard management communication with its Firefly Host VMs, disable IPv4. On the displayed list for the IPv4: box, select **Disabled**.

How you configure addressing for the Firefly Host Dashboard management center affects its communication with its Firefly Host VMs in the following way:

- In an environment in which both the Firefly Host Dashboard and the Firefly Host VM are configured for dual stack, communication problems between the Firefly Host Dashboard management interface and that of the Firefly Host VMs should not occur.
- In an environment in which the Firefly Host Dashboard is configured for dual stack but one or more of the Firefly Host VMs is not, communication problems between their management interfaces should not occur.
- In an environment in which the Firefly Host Dashboard is not configured for dual stack but all of the Firefly Host VMs are, communication problems between their management interfaces should not occur.
- In an environment in which neither the Firefly Host Dashboard nor one or more Firefly Host VM is configured for dual stack, in any case in which the IP address type of the management interfaces of the Firefly Host Dashboard and the Firefly Host VM differ—one might belong to the IPv6 protocol family and the other to the IPv4 protocol family—communication problems will occur. The Firefly Host Dashboard will not be able to connect to the Firefly Host VM to carry out any procedures.

You can make these changes during the installation process, as shown [Figure 42 on page 67](#), or you can make them later, after you complete the initial configuration.

Figure 42: Configuring Network Settings for the Firefly Host Dashboard

Wizard Progress

1. Introduction
2. Change Default Password
3. **Network Setup**
4. Time Configuration
5. Product License
6. Virtual Center Settings
7. Reports
8. Firefly Host VM Template Selection
9. Summary

Please configure the network settings for the Firefly Host management server.

The Firefly Host Dashboard IP address must stay the same, to allow the Firefly Host firewalls to be managed. It is recommended to use a static IP address so it doesn't change.

Network Configuration

Please specify fully qualified domain name (e.g. DashboardFireflyHost.company.com)

Host Name:

DNS Settings: ☒ Use DHCP to Get DNS

Primary DNS Server:

Secondary DNS Server:

Search Domain:

Interface 1

IPv4: IPv6:

IP Address:

Netmask: prefix

Default Gateway:

MAC Address:

[Prev Step](#) [Next Step](#)

In the latter case, you use the Settings module Appliance Settings > Network Settings page, which is the same page shown in [Figure 42 on page 67](#), only it is arrived at differently. For additional details, see *Configuring the Firefly Host Network Settings*.



NOTE: If you changed the IP address, you must log in to the system again. Changes to the IP address take effect immediately.

6. Set the system time.

Set the correct time zone, and then specify the NTP servers for your environment. See [Figure 43 on page 68](#).

Firefly Host components require that the correct system time be set on all ESX/ESXi hosts.

- If you do not have an NTP server, you can use a predefined server.
- If you do not have outbound Internet access to contact the NTP servers and you do not have an internal NTP server, then you must clear all entries shown in this window and set the time manually.

To do this, you use the Firefly Host CLI that you run from the vCenter console.

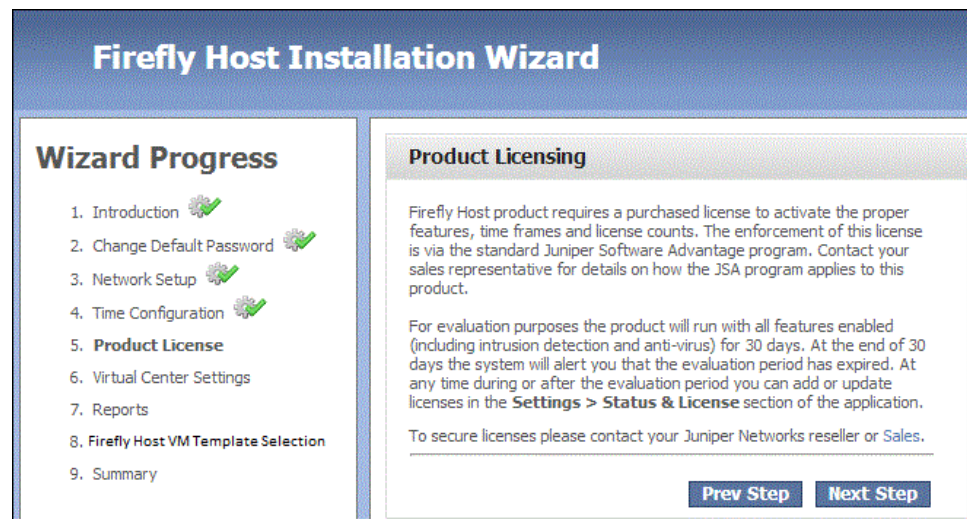
Figure 43: Configuring the Time Server

The screenshot shows the 'Wizard Progress' on the left with steps 1 through 9. Step 4, 'Time Configuration', is highlighted. The main area shows a message: 'To ensure accurate reporting of network activity, it is important to configure a time server to be server.' Below this is the 'Time Configuration' form. It includes a 'Select Timezone:' dropdown menu set to 'US/Pacific'. There are four NTP Server fields: NTP Server 1 (0.altor.pool.ntp.org), NTP Server 2 (1.altor.pool.ntp.org), NTP Server 3 (2.altor.pool.ntp.org), and NTP Server 4 (empty). At the bottom are 'Prev Step' and 'Next Step' buttons.

At this point, the wizard determines if the database disk was created and initialized properly. If you have not defined the database disk properly, the wizard displays a message.

The next screen explains Product Licensing. On the installation wizard, there is no option to enter purchased license information directly. See [Figure 44 on page 69](#).

Figure 44: Firefly Host Installation Wizard displaying Product Licensing



Click **Next Step**.

Licenses can be added after wizard completion. For additional information on Firefly Host licenses, see

- *Understanding Licenses for Firefly Host*
- *Viewing Status and License Information Using the Firefly Host Settings Module*
- *Adding and Managing Firefly Host Licenses*

7. Select the management domain, or scope, for this Firefly Host Dashboard to manage, and verify that the Firefly Host Dashboard can establish a connection to vCenter. Then click **Next Step**.

For the Firefly Host to query the vCenter for the VM inventory and other operations, you must have an account with read/write access.

- If the connection works properly, a message appears stating that the login was successful, and it identifies the number of ESX/ESXi hosts and VMs that were discovered.
- If there is a connection issue, you are notified. In that case, ensure that you have the correct credentials and that IP connectivity to the vCenter exists.

In some cases, you may need to insert another vNIC into the Firefly Host Dashboard. You must connect that vNIC to the network that connects to the vCenter server.

To configure a management domain:

- If this Firefly Host Dashboard will manage all of the vCenter's resources, select **Entire vCenter**.
- If this Firefly Host Dashboard will participate in a Split-Center configuration, select the data centers or the host clusters for this Firefly Host Dashboard to manage. To select host clusters, first select the data center that the host clusters belong to.

For information on Split-Center and its configuration options, see *Understanding the Firefly Host Split-Center Feature*.

Figure 46 on page 71 shows that this Firefly Host Dashboard is configured to manage two host clusters in Datacenter-B.

Figure 45: Firefly Host Dashboard vCenter Integration

The screenshot displays the Firefly Host Dashboard's vCenter Integration configuration page. The interface includes a top navigation bar with icons for Home, Network, Firewall, IDS, Intrusion, Compliance, Reports, and Settings. A left sidebar contains a tree view for Application Settings (Status & License, vCenter Integration, Multi-Center, Installation, Install Settings, Administrators, Active Directory, Machines, High Availability, E-Mail and Reporting, Registry Values), Security Settings (Global, Firefly Host VM Settings, IDS Settings, IDS Signatures, Alerting, Protocols, Groups, Networks, SRX Zones), and Appliance Settings (Updates, Network Settings, Proxy Settings). The main content area is divided into several panels:

- vCenter Settings:** Contains fields for Server Name or IP Address (172.30.169.35), Username (vlt-trunk), and Password (masked). A warning message states: "Notice! Changing vCenter Settings is not recommended while performing any configuration action that interacts with the vCenter, such as install, uninstall, or update of the Firefly Host or a firewall." Below these fields is a 'Select a scope for your Firefly Host' section with radio buttons for 'Entire vCenter' (selected), 'Datacenters', and 'Clusters'. A 'Save' button is at the bottom.
- Deleted VMs and Groups:** Includes a checkbox for 'Hide deleted VMs from view in the Inventory Tree' and a 'Delay before purging deleted VMs and Groups' set to 30 days. A 'Save' button is at the bottom.
- Automatic Startup:** Features a checkbox for 'Automatic Firefly Host management server and Security VM startup' and a 'Save' button.
- Update VMs:** Contains a checkbox for 'Update IP addresses as they change in vCenter' and an 'Update' button.
- Firefly Host management server plugin:** Includes 'Register' and 'Unregister' buttons.
- Synchronize machine name:** Features a checkbox for 'Sync name with vCenter' and a 'Save' button.

Figure 46: Configuring the Firefly Host Dashboard vCenter Settings

Firefly Host Installation Wizard

Wizard Progress

1. Introduction
2. Change Default Password
3. Network Setup
4. Time Configuration
5. Product License
6. **Virtual Center Settings**
7. Reports
8. Firefly Host VM Template Selection
9. Summary

vCenter Settings

Establish connection to vCenter. [more](#)

Server Name or IP Address:

Username:

Password:

Select a scope for your Dashboard Firefly Host. [more](#)

☐ Entire vCenter ☐ Datacenters ☒ Clusters

Datacenter:

☒ 10.159.24.183 (Host)

☒ 10.159.24.176 (Host)

[Prev Step](#) [Next Step](#)

8. (Optional) Configure the e-mail server to use to send reports.

Using this option, you can configure Firefly Host to send reports on system activity through e-mail. Additionally, you can configure basic information used in the report, such as the subject and the content of standard report e-mail. After you configure these parameters, you can test the e-mail connection.

You can also use the Settings module Firefly HostApplication Settings > E-Mail and Reporting page to configure this information after the installation is completed.

9. Define a template to use to instantiate Firefly Host VMs on ESX/ESXi hosts to secure them.

If you have not downloaded the Firefly Host VM and converted it to a template, do so now. You can define how the Firefly Host responds when a VM tries to connect to an ESX/ESXi host on which the Firefly Host module cannot be loaded or is not present.

You can define whether monitoring is used. Unless you plan to deploy the product in monitor mode, leave the Monitoring-only option for VMsafe unchecked. Also, unless you want to drop network traffic to VMs when the Firefly Host fails to load, you should leave the default option of **Allow All traffic** selected. You can change this option later if you want to change the behavior for one or more VMs.

10. Click **Done** to complete the Firefly Host Dashboard setup.

The Firefly Host Dashboard appears. You use this module to deploy Firefly Host VMs to the ESX/ESXi hosts to be secured, to configure other Firefly Host features, and to view specific and summary results information and reports.

- Related Documentation**
- [Preparing to Integrate Firefly Host with the VMware Environment on page 43](#)
 - [Understanding Firefly Host on page 3](#)
 - *Understanding the Firefly Host Settings Module*
 - [Understanding the Firefly Host Main Module on page 17](#)

PART 4

Firefly Host Settings Infrastructure to Secure Hosts

- [Securing ESX/ESXi Hosts using Firefly Host on page 75](#)
- [Firefly Host Firewall Module on page 79](#)
- [Firefly Host Network Module on page 109](#)

CHAPTER 8

Securing ESX/ESXi Hosts using Firefly Host

- [Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard on page 75](#)
- [Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured on page 76](#)
- [Understanding Automatic Securing of VMs on page 77](#)

Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard

After you install the Firefly Host VM on an ESX/ESXi host to secure it, the Firefly Host Dashboard allows you to manually secure virtual machines (VM) on that host or remove them from the protected network. Removing a secured VM from the protected network is referred to as *unsecuring* the VM.

To secure a VM that does not belong to the Secured Network:

1. In the Firefly Host Dashboard Settings module Firefly Host Application Settings section, select **Installation**.
2. In the Unsecured Network pane, select the VM that you want to secure. Click the check box in front of its name.
3. Click **Secure**.

As it secures the VM, the Firefly Host reports on the status of each part of the process. If the VM is successfully secured, the report states that the VM was successfully secured.

4. Click **Close**.

The Firefly Host Dashboard displays a process symbol that dynamically indicates that the VM is being secured with a firewall and moved into the secured network. The VM is now protected, and it appears in the Secured Network pane.

After all Firefly Host components in your environment are upgraded to release 6.0, if you attempt to introduce components from a previous release, the process is halted and Firefly Host displays a message informing you that you must install the correct version.

Related Documentation

- [Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured on page 76](#)
- [Installing Firefly Host VMs on ESX/ESXi Hosts](#)
- [Understanding Firefly Host on page 3](#)

Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured

You use the Firefly Host Dashboard Settings module Installation section to secure and unsecure a VM. By default, the Firefly Host suspends and resumes a VM when you unsecure it. You can change this behavior by changing the value of the `vm-safe.config` option.

- [Displaying the State of the `vm-safe.config` Setting on page 76](#)
- [Disabling the Suspend-Resume Process on page 76](#)

Displaying the State of the `vm-safe.config` Setting

This example shows the default setting. You can use the following command to display the current state of the `center.config vm-safe.config` option:

```
(Cmd) config show center.suspend.after.vmsafe.config
# whether center should suspend and resume VM after VMsafe configuration
center.suspend.after.vmsafe.config = true
```

Disabling the Suspend-Resume Process

In some cases it might be necessary or desirable to stop Firefly Host from enacting the suspend-resume process after a VM is unsecured. For example, you might want to disable the process to allow the VM to be migrated to another host or to suspend and resume the VM later after completing the removal of protection from the VM.



TIP: Take care when you protect VMs such as the VMware vCenter Database VM and other VMs that must not be suspended.

To enable the `vm-safe.config` process to take effect after the VM is migrated to another host without suspending the VM, use the following statement. Set the option to `false` in `center.config`:

```
(Cmd) config set center.suspend.after.vmsafe.config false
```

After changing this value, either restart the Firefly Host management process or reboot the Firefly Host Dashboard. You can use the service restart command line or the Firefly Host Dashboard to restart the Firefly Host management process.

To restart the Firefly Host management process from the command line, enter the following command:

```
(Cmd) service restart tomcat
Sending 'restart' command
The following watches were affected:
```


tomcat

To restart the Firefly Host management process using the Firefly Host Dashboard:

1. Select the Settings module Support section.
2. In the Restart pane of the displayed page, click **Restart**.

Related Documentation

- [Installing Firefly Host VMs on ESX/ESXi Hosts](#)
- [Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard on page 75](#)
- [Understanding Firefly Host on page 3](#)

Understanding Automatic Securing of VMs

Firefly Host allows you to configure your system to *automatically* secure VMs. Auto-securing VMs streamlines policy application allowing you to efficiently ensure security throughout your virtual infrastructure. You can configure the Auto-Secure feature options to direct Firefly Host to automatically secure VMs in the manner most appropriate for your environment.

You use the Settings module Firefly Host Application Settings > Install Settings > Automatic Securing of VMs pane to configure Auto-Secure for your virtualized environment.

The Automatic Securing of VMs pane includes the following options:

- No VM

No individual VMs or groups of VMs are automatically secured. This is the default behavior.

- VMs in the following group

This option allows you to select either a Static Group or a Smart Group from the list of existing groups. The list contains all groups, including those configured as Policy Groups and those that are not. Using this option, you can select only one group.



NOTE: Only VMs in the selected group are automatically secured.

- If you did not configure the selected group as a Policy Group, Firefly Host automatically secures members of the group with the Global and Default policies.
- If you configured the selected group with the Policy Group option, then any policy rules that were created for the group and applied to it take effect. In this case, the Default policy is not used.
- VMs with a VM Policy or in a Policy Group

Because Default Policy and Global Policy rules tend to be restrictive, they are not appropriate for securing all VMs. This option allows you to predefine policy rules for individual VMs and groups of VMs and direct Firefly Host to use the policy rules that

you predefined to automatically secure them rather than relying on just the Default and Global policy rules. Using this option, you can automatically secure many Policy Groups and individual VMs instead of being restricted to selecting a single group.

VMs that fit any of the following criteria are automatically secured:

- Individual VMs for which you have predefined specific policy rules and applied those policies using the Firewall module Apply Policy page to install the policy.
- Groups of VMs that you created as Static Groups or Smart Groups and for which you selected the Policy Group option. You must also have created and applied a policy for the group, and that policy must contain rules.
- All VMs

All VMs are automatically secured. As described previously, any policy rules defined for Policy Groups that have been previously applied take effect for VM members of the group. If a VM is not a member of any group, then Global and Default Policies and any individual VM rules take effect for them.

You can refine this selection by excluding a specific group of VMs.

- Optionally, exclude a group of VMs from being automatically secured. You might want to exclude VMs from auto-securing that you are using for testing.



NOTE: Firefly Host auto-secure feature will not attempt to secure an FT-enabled VM. Firefly Host generates an alert telling you that you must disable FT for that VM or suspend the VM for Firefly Host to secure the VM. The auto-secure feature monitors for cases in which an FT-enabled VM is disabled and for VMs that are suspended and powered-off.

If a VM is automatically secured, you cannot use the Settings module Installation page to unsecure it. The VM is shown on this page in a dimmed box and a message is presented informing you that it is automatically secured. In this case, if you were able to unsecure the VM, Firefly Host would simply secure it again automatically.

Instead, you must first remove the VM from the automatically secured group that it belongs to, or, if it is an individual VM, remove the policy from it, and then unsecure it.

**Related
Documentation**

- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host VM on page 24](#)

CHAPTER 9

Firefly Host Firewall Module

- [Understanding the Firefly Host Firewall Module on page 79](#)
- [Understanding How Firefly Host Handles ICMPv6 Protocol Traffic on page 93](#)
- [Understanding Predefined Objects for Firefly Host Firewall Policy Terms on page 97](#)
- [Configuring Firefly Host Firewall Policies on page 100](#)
- [Understanding Firefly Host Predefined Firewall Policy for Its Components on page 107](#)

Understanding the Firefly Host Firewall Module

This topic covers the Firefly Host 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.

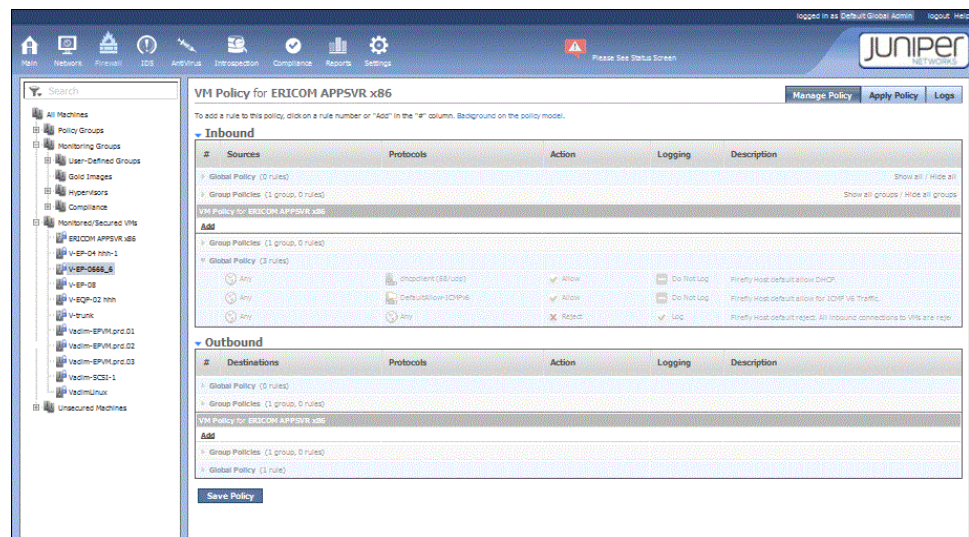
This topic contains the following sections:

- [The Firewall Module and the VM Tree on page 79](#)
- [Overview of the Firewall Policy Model on page 80](#)
- [Global Policy, Group Policy, and Individual VM Policy Tiers on page 81](#)
- [Firewall Policy Structure and Policy Rules Precedence on page 84](#)
- [Viewing the Complete Policy Rule Base for a VM on page 86](#)
- [The Manage Policy Tab on page 86](#)
- [The Apply Policy Tab on page 90](#)
- [The Logs Tab on page 92](#)

The Firewall Module and the VM Tree

The Firewall module of the Firefly Host Dashboard 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 47 on page 80](#) shows information for a single VM.

Figure 47: 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 Firefly Host 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 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 Firefly Host 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 Firefly Host 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 Firefly Host 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. Firefly Host 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 Firefly Host 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 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 Firefly Host 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.

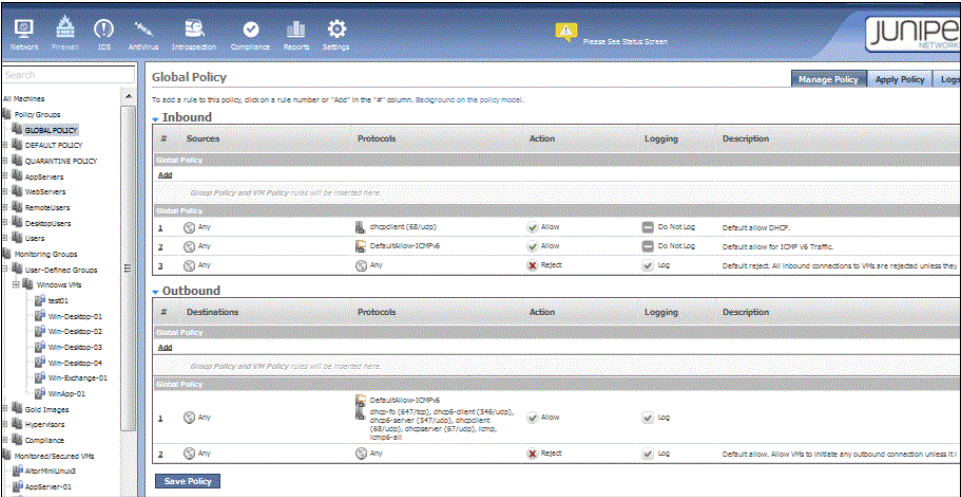
- Low-level Global Policy rules

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 48 on page 83](#) is displayed.

Figure 48: 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.

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 a group policy associated with it is automatically assigned the Default Policy. Later if it becomes a member of a policy group, then it inherits that group's Group Policy rules, and the Default Policy rules no longer apply.

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 Firefly Host 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.

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 Firefly Host 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

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.

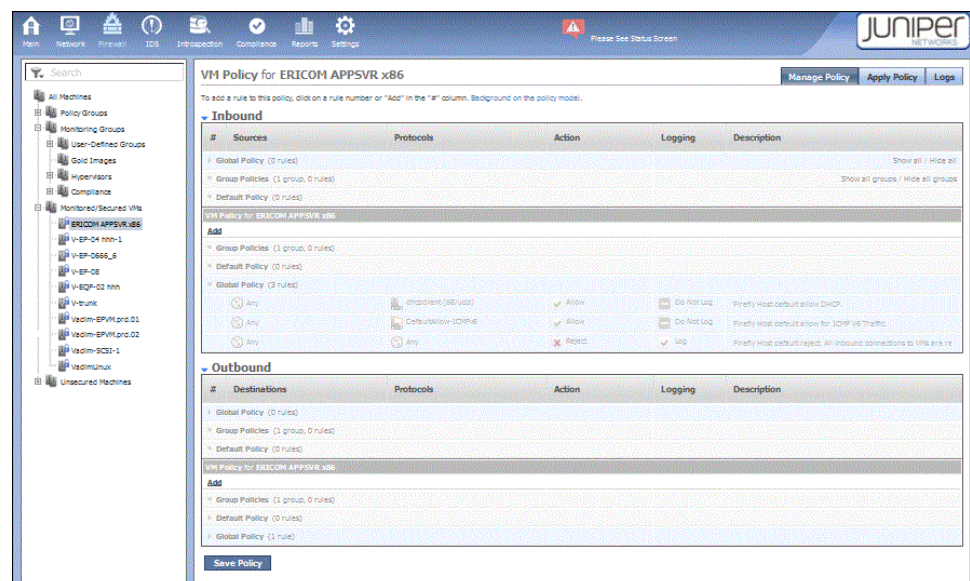
To ensure that you always have management access, you could affect the precedence in the policy for any VM that belongs to that group by moving the rule that allows management access up from the low-level Group Policy section to the high-level Group Policy section. To do so, click the rule number in 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 Firefly Host 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 49 on page 86](#).

Figure 49: VM Policy Expanded Rule Base

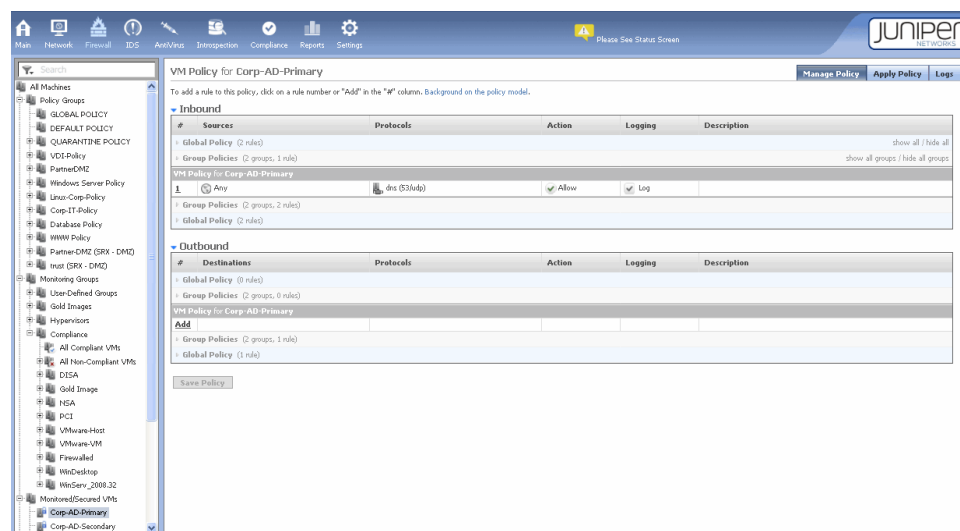


The Manage Policy Tab

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

object in the VM tree. You can select all machines, a group, or an individual VM. [Figure 50 on page 87](#) shows the policy for the Corp-AD-Primary VM.

Figure 50: Firewall Module Manage Policy Page



This section contains the following parts:

- [Policy Per vNIC and Dual Stack on page 87](#)
- [Creating a Policy Rule on page 87](#)

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.

Firefly Host 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.

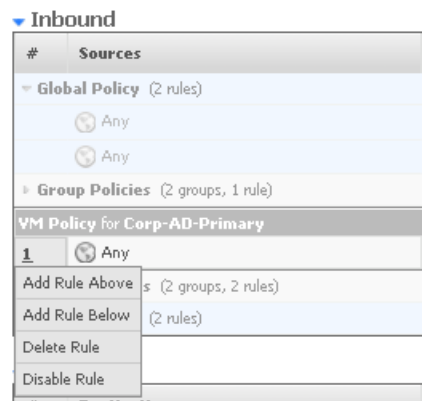
Using the Policy per vNIC feature, you can handily apply different policy rules to vNICs passing IPv4 traffic from those used for IPv6 traffic even when the vNICs are attached to the same VM. To apply the rule to all traffic of a type, you could use the predefined terms **Any-IPv4** and **Any-IPv6**.

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 51 on page 88](#).

Figure 51: Adding a Rule



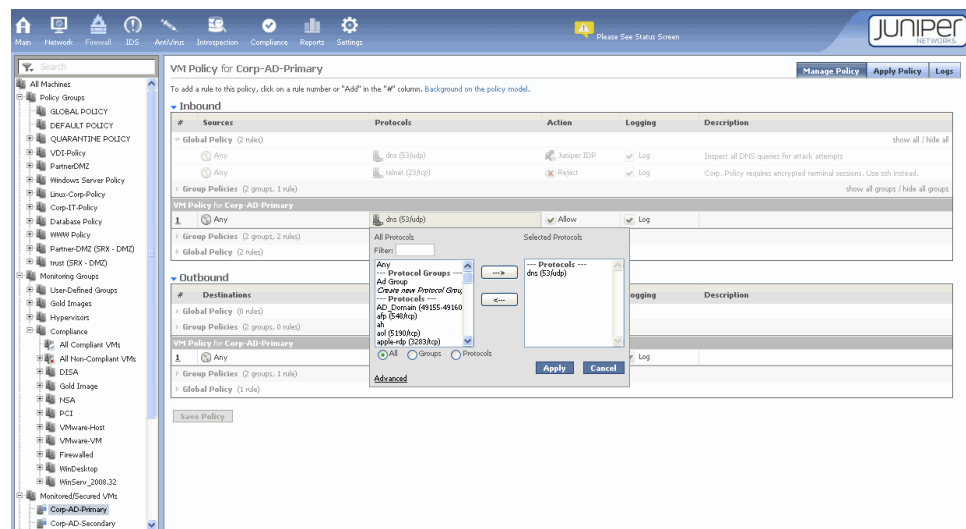
NOTE: Rules are applied in order of execution from top to bottom.

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 52 on page 88](#).

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

Figure 52: Using the Dialog Box Filter to Add Terms for policy rules



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

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 Firefly Host Dashboard 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 8 on page 89 describes the policy configuration settings.

Table 8: 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 <i>Configuring Global Settings Using the Firefly Host Settings Module (VMware)</i> .
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 Firefly Host to send e-mail messages or SNMP traps. See “Alerts” on page 80.
Description	Enter a description for the policy.

The Apply Policy Tab

The Apply Policy tab allows you to push security policies out to the Firefly Host 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 Firefly Host VM that protects the VM.
- The date that the policy was installed.

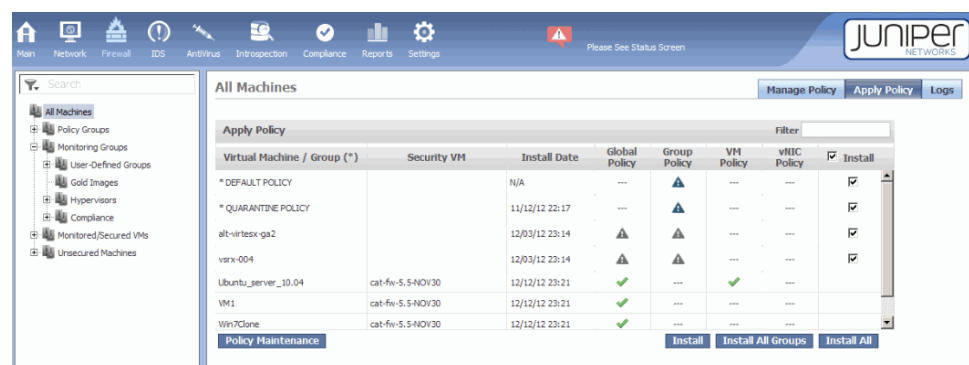
To install a policy on one or more selected VMs:

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**.

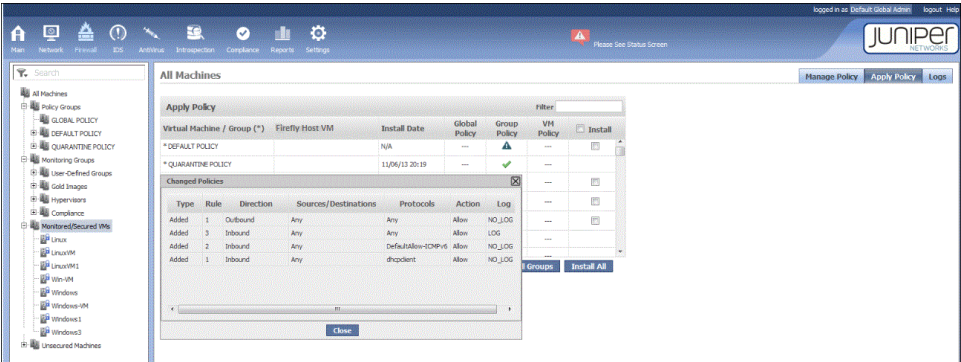
Figure 53 on page 90 shows the Apply Policy page.

Figure 53: Firewall Apply Policy Page








Click on warnings to view the changed policy rules. See [Figure 54 on page 91](#).

Figure 54: Changed Policies Dialog Box



See [Table 9 on page 91](#) for a list of icons displayed for VMs on the Apply Policy page.

Table 9: 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 Firefly Host VM firewall. This usually indicates an error condition that you should investigate.
	<p>The policy type does not exist for the VM. For example, an individual VM policy for that VM is not configured.</p> <p>You are not required to build individual VM policies for each VM.</p>
	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 55 on page 92 shows the Logs tab.

For the Logs tab, you can use an advanced option that includes a mark verified VMs setting. Firefly Host 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 55: Firewall Module Logs Tab

Start Time	Rule Id	Action	Source	Source Port	Destination	Proto	IP Proto	Record Id
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46990/tcp	Partner-Web-eConn	mysql	tcp	19399997
09/02/11 10:47	5	Reject	VDI-Workstation2	65100/tcp	WWW-TT-1	http	tcp	19399996
09/02/11 10:47	5	Reject	VDI-Workstation2	65100/tcp	WWW-TT-1	http	tcp	19399995
09/02/11 10:47	5	Reject	VDI-Workstation2	65099/tcp	WWW-TT-1	http	tcp	19399994
09/02/11 10:47	5	Reject	VDI-Workstation2	65099/tcp	WWW-TT-1	http	tcp	19399993
09/02/11 10:47	5	Reject	VDI-Workstation2	65099/tcp	WWW-TT-1	http	tcp	19399992
09/02/11 10:47	5	Reject	VDI-Workstation2	65098/tcp	WWW-TT-1	http	tcp	19399991
09/02/11 10:47	5	Reject	VDI-Workstation2	65098/tcp	WWW-TT-1	http	tcp	19399990
09/02/11 10:47	2	Allow	Partner-Web-eConn	54391/tcp	Partner-SQL-eConn	mysql	tcp	19399989
09/02/11 10:47	2	Allow	Partner-Web-eConn	54390/tcp	Partner-SQL-eConn	mysql	tcp	19399988
09/02/11 10:47	2	Allow	Partner-Web-eConn	54389/tcp	Partner-SQL-eConn	mysql	tcp	19399987
09/02/11 10:47	2	Allow	Partner-Web-eConn	54388/tcp	Partner-SQL-eConn	mysql	tcp	19399986
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43672/tcp	Partner-Web-eConn	http	tcp	19399985
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43671/tcp	Partner-Web-eConn	http	tcp	19399984
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43670/tcp	Partner-Web-eConn	http	tcp	19399983
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43669/tcp	Partner-Web-eConn	http	tcp	19399982
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43668/tcp	Partner-Web-eConn	http	tcp	19399981
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46984/tcp	Partner-Web-eConn	mysql	tcp	19399980
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46983/tcp	Partner-Web-eConn	mysql	tcp	19399979
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46982/tcp	Partner-Web-eConn	mysql	tcp	19399978
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46981/tcp	Partner-Web-eConn	mysql	tcp	19399977
09/02/11 10:47	29	Allow	Partner-Web-eConn	54391/tcp	Partner-SQL-eConn	mysql	tcp	19399976
09/02/11 10:47	29	Allow	Partner-Web-eConn	54390/tcp	Partner-SQL-eConn	mysql	tcp	19399975
09/02/11 10:47	29	Allow	Partner-Web-eConn	54389/tcp	Partner-SQL-eConn	mysql	tcp	19399974
09/02/11 10:47	29	Allow	Partner-Web-eConn	54388/tcp	Partner-SQL-eConn	mysql	tcp	19399973
09/02/11 10:47	33	Allow	Partner-SQL-eConn	43672/tcp	Partner-Web-eConn	http	tcp	19399972
09/02/11 10:47	33	Allow	Partner-SQL-eConn	43671/tcp	Partner-Web-eConn	http	tcp	19399971
09/02/11 10:47	33	Allow	Partner-SQL-eConn	43670/tcp	Partner-Web-eConn	http	tcp	19399970

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 Firefly Host Policy per vNIC Feature](#)
- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [About the Firefly Host Dashboard Tree on page 30](#)
- [Understanding the Firefly Host Network Module on page 109](#)
- [Understanding Firefly Host on page 3](#)

Understanding How Firefly Host 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 Firefly Host default firewall policy protocol group for handling ICMPv6 traffic.



WARNING: By default Firefly Host 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 93](#)
- [Filtering ICMPv6 Packets on page 93](#)
- [Default Policy Group for Allowing Inbound ICMPv6 Packets on page 94](#)

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.

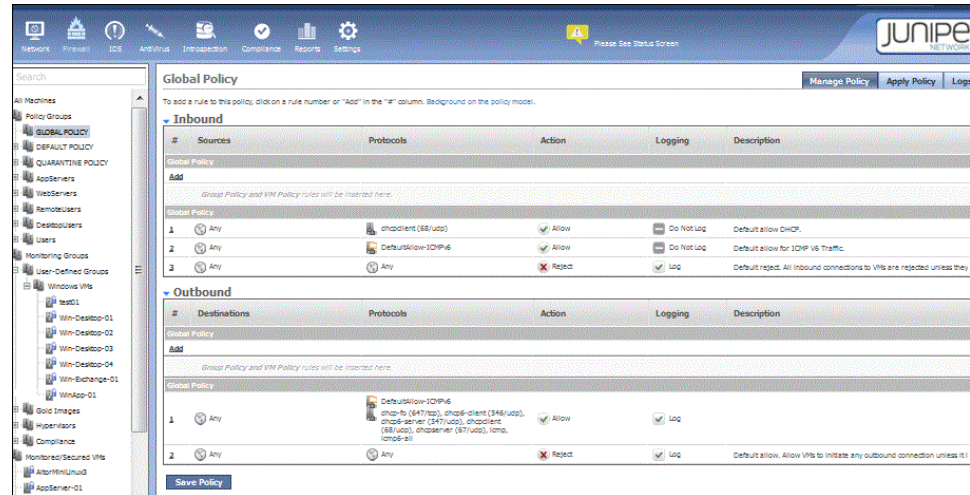
ICMP for IPv4 is an auxiliary protocol not necessarily required for IPv4 proper functioning. By contrast, ICMPv6 is an essential component in the establishment and maintenance of IPv6 communications. Among the messages it includes are those for address assignment, address resolution, and multicast group 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.

Firefly Host 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 56 on page 94](#).

Figure 56: Default Global Policy Showing Default ICMPv6 Allow Group



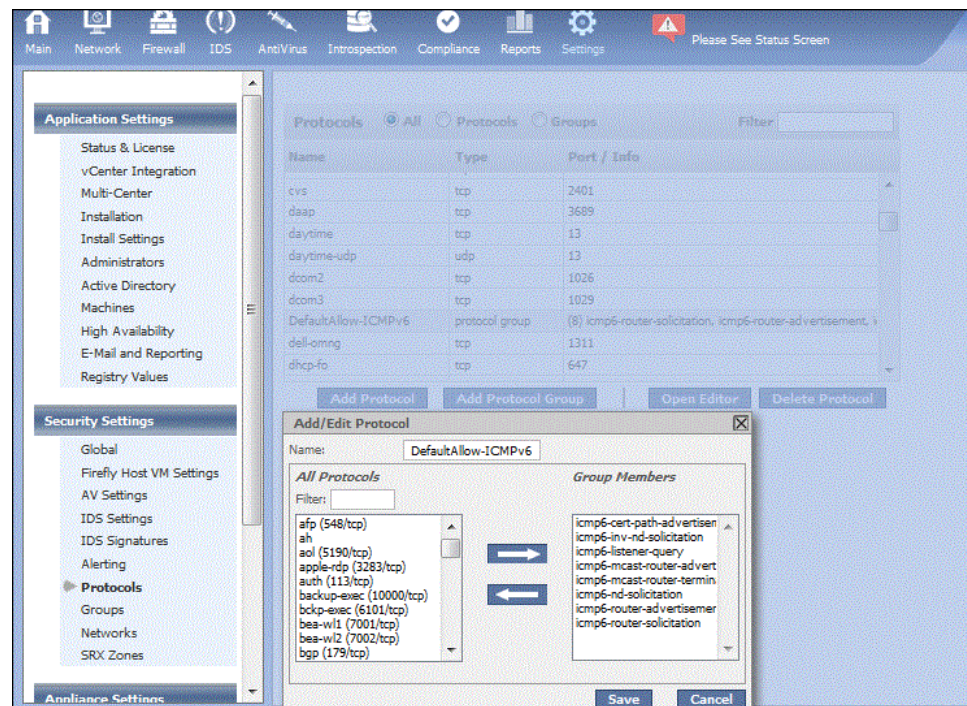
Default Policy Group for Allowing Inbound ICMPv6 Packets

Firefly Host 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 ICMPv6 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 96](#).

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 57 on page 95](#).

Figure 57: Protocols Settings ICMPv6 Default Protocol Group



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 Firefly Host 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
- 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 Firefly Host Firewall Module on page 79](#)
- [Understanding Firefly Host Predefined Firewall Policy for Its Components on page 107](#)
- [Understanding Firefly Host IPv6 Support](#)
- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host Settings Module](#)

Understanding Predefined Objects for Firefly Host Firewall Policy Terms

This topic focuses primarily on the Firefly Host 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 97](#)
- [Predefined Global IP Address Objects on page 97](#)
- [Predefined Network Objects on page 98](#)

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.

Firefly Host 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 Firefly Host Dashboard 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 Firefly Host Dashboard.

- You can select a network or a machine that you have already defined.
- You can select any of the predefined objects that Firefly Host provides. The following sections cover these objects.

Predefined Global IP Address Objects

Firefly Host Release 6.0 introduces support for IPv6, including configuration of policies on IPv6 traffic. Firefly Host 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 6.0—releases before Firefly Host supported IPv6—the term Any referred to any IPv4 address. For environments in which not all Firefly Host components are at version 6.0 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 Firefly Host components environments, see *IPv6 Support in Homogeneous and Heterogeneous Firefly Host Environments*.



WARNING: All Firefly Host components must be at version 6.0 or later for you to be able to create policies on IPv6 traffic.

Predefined Network Objects

Firefly Host 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 Firefly Host Release 6.0, you used the Settings module Security Settings > Global Settings Rules pane to control broadcast and multicast settings. As of Release 6.0, 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.

Predefined Network Objects for Well Known IP Addresses

Firefly Host 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 IETF 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 IETF 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: Firefly Host accepts both IPv4 and IPv6 address formats and displays the addresses as you enter them.

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

The IETF 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 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 IETF 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 IETF 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 IETF 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 IETF 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 **flags** 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 Firefly Host Firewall Module on page 79](#)
- [Configuring Firefly Host Firewall Policies on page 100](#)
- [Understanding the Firefly Host Policy per vNIC Feature](#)
- [Understanding Firefly Host on page 3](#)

Configuring Firefly Host 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 Firefly Host Firewall Module on page 79](#)”. 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.

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

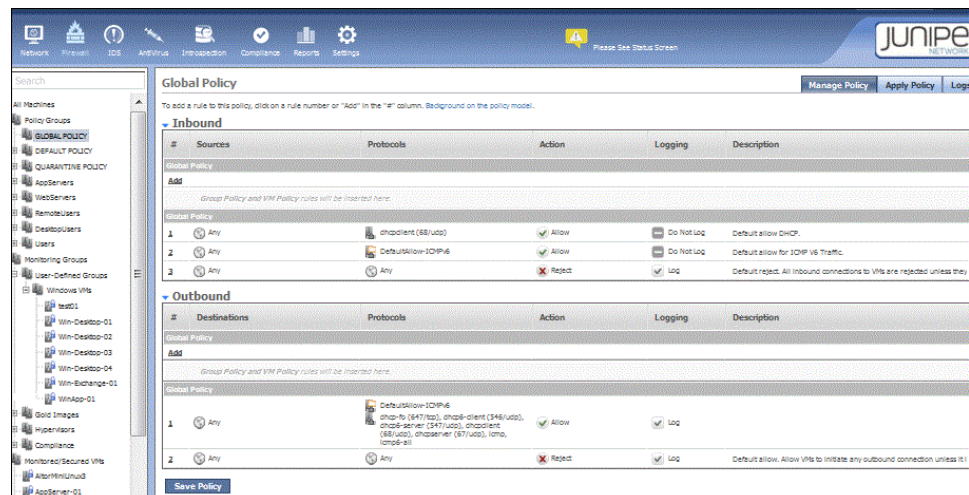


NOTE: This example focuses on defining an inbound policy only. The process of defining outbound policy mirrors it.

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

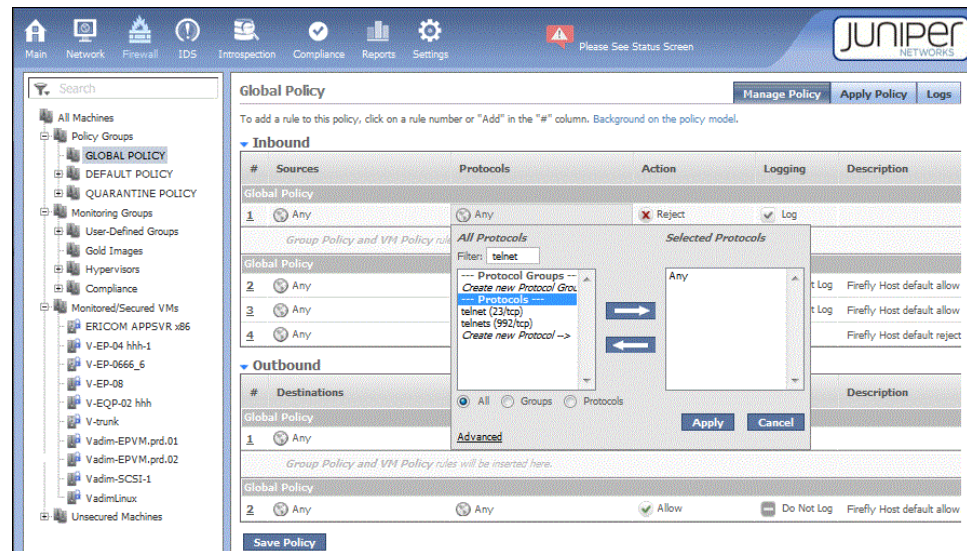
The Global Policy page appears. It contains Inbound and Outbound sections. Each section contains a high-level Global Policy section and a low-level Global Policy section with a placeholder for Group Policy rules and individual VM Policy rules in the middle. [Figure 58 on page 102](#) shows the Global Policy with its default policy rules.

Figure 58: 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 59 on page 103](#).

Figure 59: 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 Firefly Host 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**.

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.



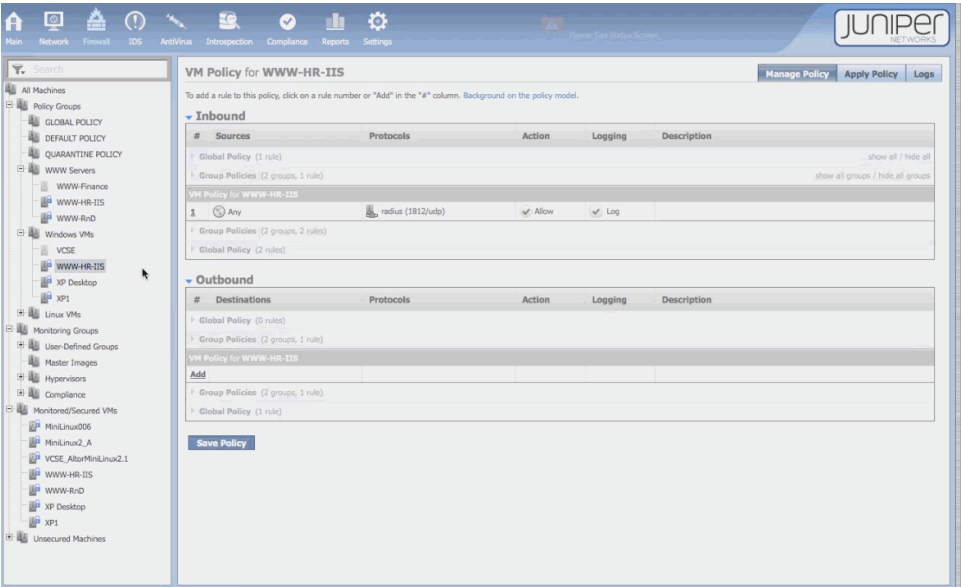
TIP: Because WWW-HR-IIS belongs to two groups, you can select it under either of its groups to display its VM Policy page.

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 60 on page 105 shows the policy.

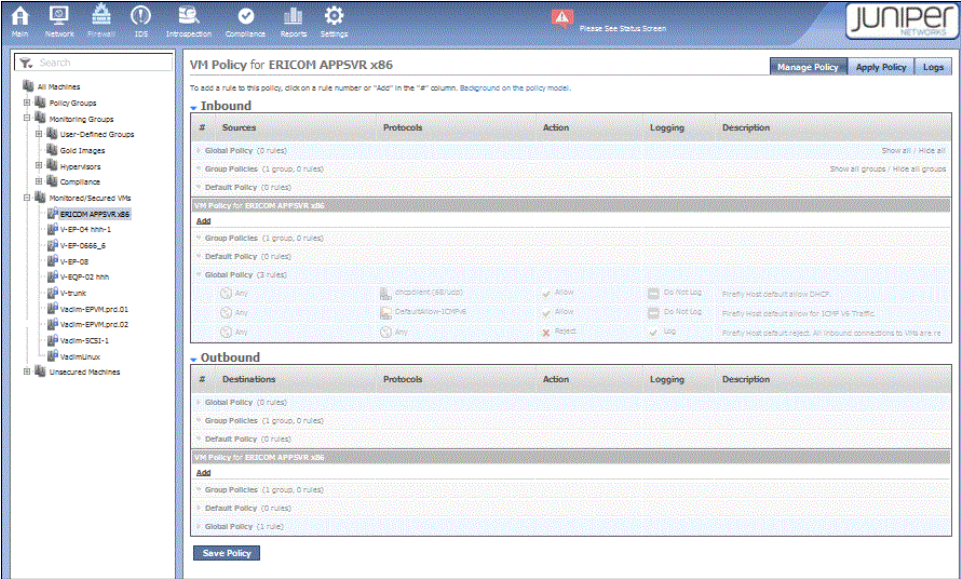
Figure 60: VM Policy for an Individual VM



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 61 on page 105](#).

Figure 61: Complete VM Policy for an Individual VM

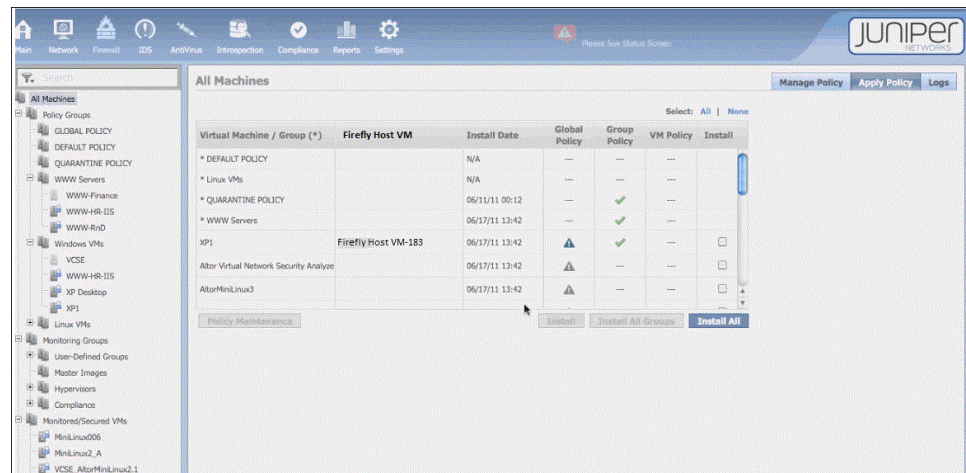


Apply the VM Policy.

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.

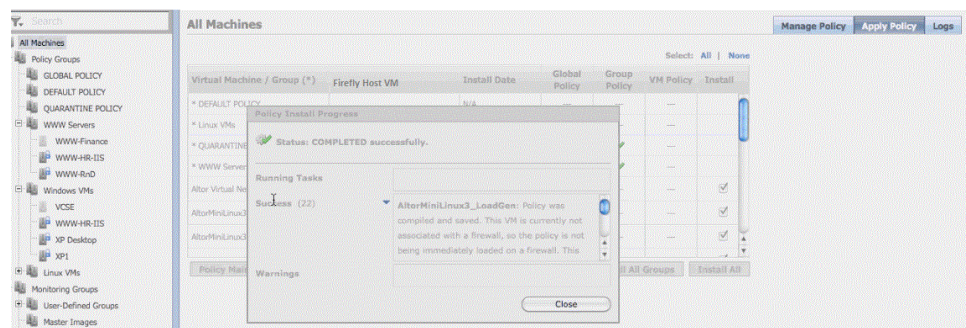
1. Select the Firewall module. Select **All Machines** in the VM Tree. The following page is displayed. See [Figure 62 on page 106](#).

Figure 62: All Machines



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. See [Figure 63 on page 106](#).

Figure 63: Policy Install Progress



Related Documentation

- [Understanding Firefly Host on page 3](#)
- [Using the Firefly Host Network and Firewall Modules Cooperatively on page 114](#)
- [Understanding Firefly Host Predefined Firewall Policy for Its Components on page 107](#)

Understanding Firefly Host Predefined Firewall Policy for Its Components

Firefly Host 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, Firefly Host secures and protects its own two main components—the Firefly Host Dashboard and the Firefly Host VM—with predefined rule sets. You cannot change these predefined policy rules nor should you ever need to.

Firefly Host stateful firewall comprises the following predefined rule sets for its two components.

For the Firefly Host Dashboard, 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 Firefly Host 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 Firefly Host Firewall Module on page 79](#)
- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host VM on page 24](#)
- [Understanding Firefly Host on page 3](#)

CHAPTER 10

Firefly Host Network Module

- [Understanding the Firefly Host Network Module on page 109](#)
- [Using the Firefly Host Network and Firewall Modules Cooperatively on page 114](#)

Understanding the Firefly Host Network Module

The Firefly Host Dashboard 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 109](#)
- [Manipulating Displayed Information on page 110](#)

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 Firefly Host Application Settings > Machines page.

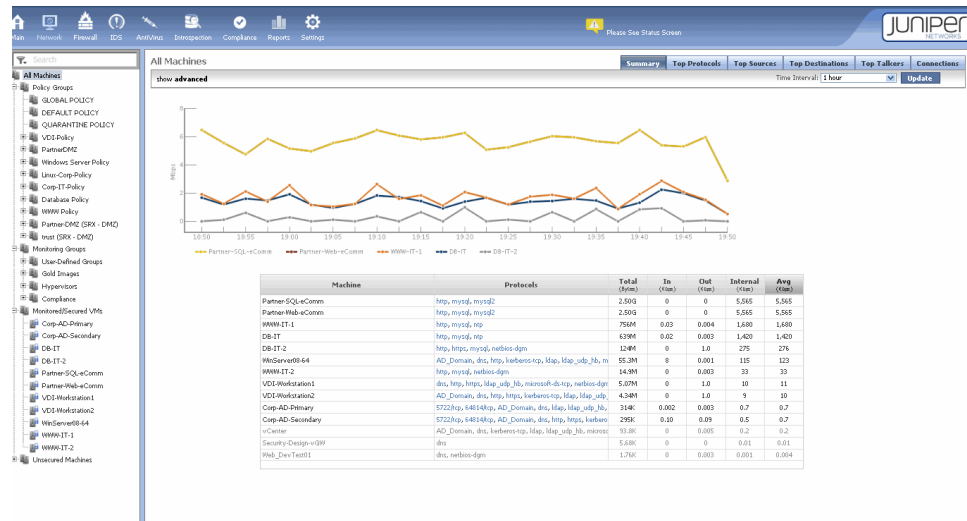
The Network module analysis takes into account IPv4 traffic and IPv6 traffic. Tables shown on the Network module tabs display information for objects with IPv4 and IPv6 addresses.

Manipulating Displayed Information

The Network Summary tab allows you to display information about all VMs, as shown in Figure 64 on page 110.

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.

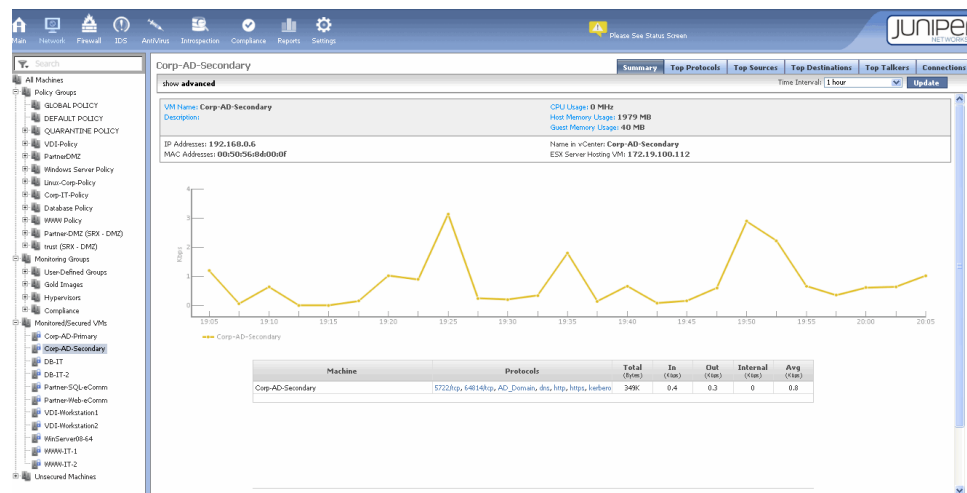
Figure 64: Network Summary Tab for All VMs



To display information about a single VM, select the VM in the VM tree.

Figure 65 on page 110 shows the information displayed for the Corp-AD-Secondary VM.

Figure 65: Main Module Network Module Summary Tab for a Single VM

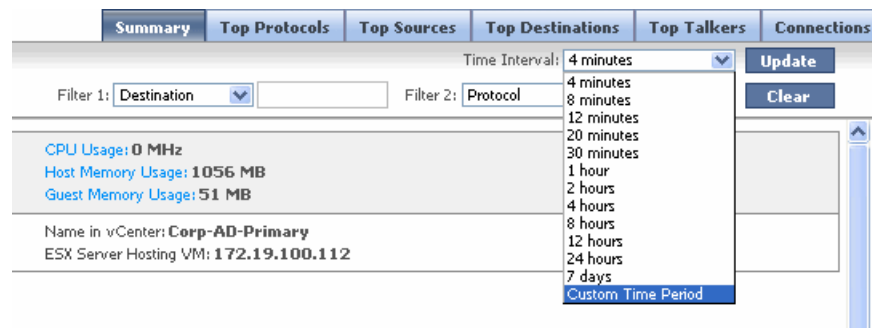


To view a VM's connections, click an individual line in the graph. To display a filter for a protocol, click the protocol field.

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 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 68 on page 112 shows the Custom Time Period menu item.)

Figure 68: Selecting a Time Interval

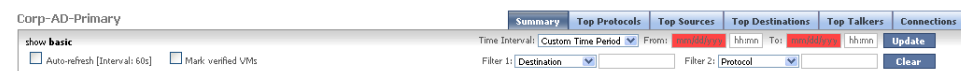


The custom time period is interpreted as follows:

- You cannot 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—Firefly Host 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, Firefly Host 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, Firefly Host uses the time you specified.

Figure 69 on page 112 shows the Custom Time Period fields.

Figure 69: 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 Firefly Host Dashboard 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.

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 10 on page 113](#) describes the Advanced options.

Table 10: Using Advanced Options for Filtering Network Data

Select	Action
Auto-refresh	Refreshes data automatically every 60 seconds.
mark verified VMs	<p>Causes the Firefly Host 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. Firefly Host reports on both IPv4 and IPv6 addresses.</p> <p>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.</p>
multicast in table	<p>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.</p> <p>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.</p>

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 Firefly Host Network and Firewall Modules Cooperatively on page 114](#)
- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [About the Firefly Host Dashboard Tree on page 30](#)
- [Understanding Firefly Host on page 3](#)

Using the Firefly Host Network and Firewall Modules Cooperatively

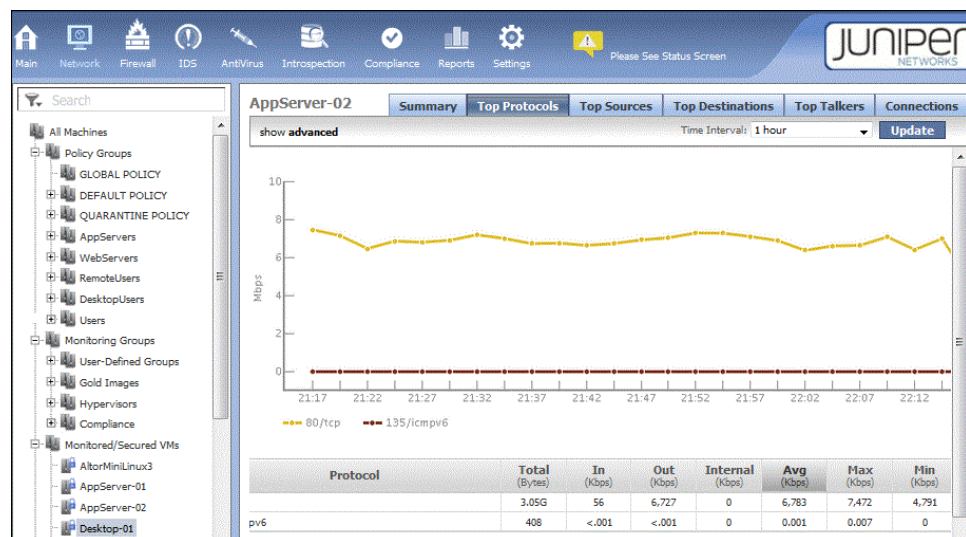
There are various ways to use the Network module in the service of the Firewall module to build a strong firewall. This topic explores some of them.

- [Network Assessment on page 114](#)
- [Using the Network Module to Observe Traffic Coming Into and Going Out from VMs on page 115](#)
- [Detecting Unexpected and Unwanted Behavior on page 115](#)
- [Using the Network and Firewall Modules Together on page 116](#)

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. Firefly Host 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 70 on page 114](#), 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.

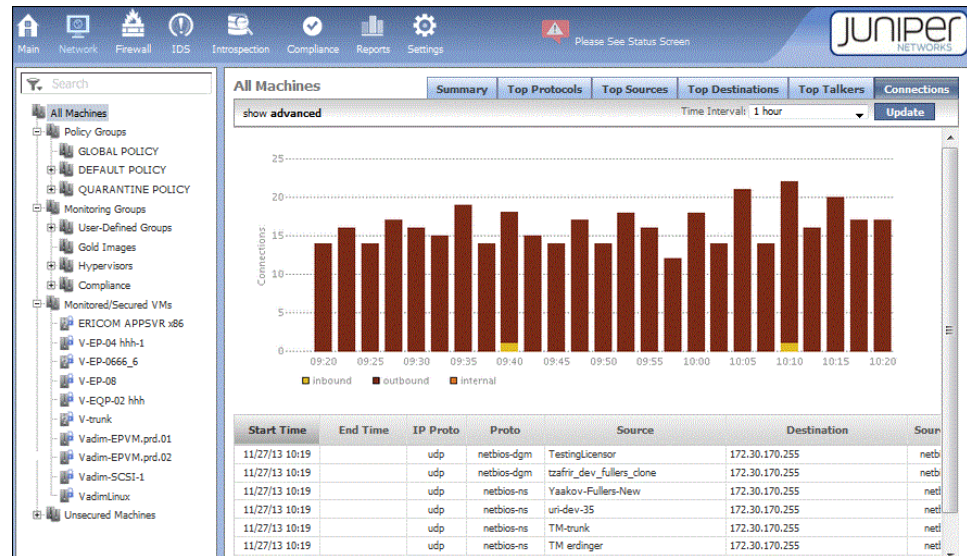
Figure 70: Top Protocols Across All Machines Example



Because the Firefly Host 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 Firefly Host ability to view connections in real time, you would still be able to make realistic network assessments. But the Firefly Host can contribute much more information to use in your network assessment.

As [Figure 71 on page 115](#) 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 71: 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, Firefly Host 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 Firefly Host Firewall Module on page 79](#)
- [Understanding the Firefly Host Network Module on page 109](#)
- [Understanding the Firefly Host Dashboard on page 11](#)
- [Understanding the Firefly Host Dashboard Taskbar on page 29](#)
- [About the Firefly Host Dashboard Tree on page 30](#)
- [Understanding Firefly Host on page 3](#)

PART 5

Index

- [Index on page 119](#)

Index

Symbols

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

B

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

C

comments, in configuration statements.....	xvii
configuring basic system parameters.....	61
conventions	
text and syntax.....	xvi
curly braces, in configuration statements.....	xvii
customer support.....	xviii
contacting JTAC.....	xviii

D

DNS services.....	39
documentation	
comments on.....	xvii

E

ESX/ESXi hosts.....	7
events and alerts.....	17

F

Firefly Host Dashboard	
Firewall module.....	79, 114
Main module.....	17
navigation.....	27
Network module.....	109, 114
overview.....	11
predefined firewall policy rules	107
taskbar.....	29

Firefly Host module.....	9
Firefly Host VM	
installation modes.....	44
overview.....	24
predefined firewall policy rules	107
single OVA install method.....	58
Firewall module.....	79
used with Network module.....	114
firewall policy rules for Firefly Host	
components.....	107
font conventions.....	xvi

H

hypervisors	
overview.....	9

I

ICMPv6P.....	93
installation	
prerequisites and resource requirements.....	39

M

Main module.....	17
manuals	
comments on.....	xvii

N

network connectivity.....	39
Network module.....	109
used with Firewall module.....	114
NTP.....	44
NTP services.....	39

O

Open Virtualization Format (OVF)	
OVA template.....	47, 48
OVA bundled method.....	48
downloading package.....	49
OVA template.....	47
OVA template method	
single method for Firefly Host Dashboard.....	56

P

parentheses, in syntax descriptions.....	xvii
port groups.....	39
Primary-level entry	
secondary-level entry.....	97
Primary-level entry only.....	97

Protocols	
ICPMv6.....	93
R	
resource requirements	
DNS services.....	39
network connectivity.....	39
NTP services.....	39
port groups.....	39
vCenter.....	39
virtual appliances.....	39
virtual devices.....	39
vNICs.....	39
vSphere.....	39
vSwitches.....	39
Web browsers.....	39
S	
security zones	
interfaces.....	61
single OVA install method	
Firefly Host VM	58
status and status icons.....	17
support, technical See technical support	
syntax conventions.....	xvi
T	
taskbar.....	29
technical support	
contacting JTAC.....	xviii
time synchronization.....	44
V	
vCenter.....	39
virtual appliances.....	39
virtual devices	
sizes.....	39
VMotion.....	7
VMsafe Firewall + Monitoring mode.....	44
VMsafe Monitoring mode.....	44
VMware.....	39
ESX/ESXi hosts.....	7
infrastructure and Firefly Host.....	7
VMotion.....	7
vSphere.....	7
vSphere operating system.....	7, 39
See also Virtual Center (vCenter)	
VMware VMsafe APIs.....	44
vNICs.....	39
vSphere.....	7
vSwitches.....	39
W	
Web browsers supported.....	39