vShield Administration Guide

vShield Manager 4.1.0 Update 1
vShield Zones 4.1.0 Update 1
vShield Edge 1.0.0 Update 1
vShield App 1.0.0 Update 1
vShield Endpoint 1.0.0 Update 1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.
Contents

About This Book   9

vShield Manager and vShield Zones

1 Overview of vShield  13
   vShield Components  13
   vShield Manager  13
   vShield Zones  13
   vShield Edge  14
   vShield App  14
   vShield Endpoint  15
   Migration of vShield Components  15
   VMware Tools  15
   Ports Required for vShield Communication  15

2 vShield Manager User Interface Basics  17
   Logging in to the vShield Manager User Interface  17
   Accessing the Online Help  18
   vShield Manager User Interface  18
      vShield Manager Inventory Panel  18
      vShield Manager Configuration Panel  19

3 Management System Settings  21
   Identify Your vCenter Server  21
   Register the vShield Manager as a vSphere Client Plug-in  22
   Identify DNS Services  22
   Set the vShield Manager Date and Time  23
   Identify a Proxy Server  23
   Download a Technical Support Log from a Component  23
   Back Up vShield Manager Data  24
   View vShield Manager System Status  24
   Add an SSL Certificate to Identify the vShield Manager Web Service  24

4 Zones Firewall Management  27
   Using Zones Firewall  27
      Default Rules  28
         Layer 4 Rules and Layer 2/Layer 3 Rules  28
         Hierarchy of Zones Firewall Rules  28
         Planning Zones Firewall Rule Enforcement  28
      Create a Zones Firewall Rule  29
      Create a Layer 2/Layer 3 Zones Firewall Rule  30
   Validating Active Sessions against the Current Zones Firewall Rules  31
   Revert to a Previous Zones Firewall Configuration  31
   Delete a Zones Firewall Rule  32
5 User Management 33
   Managing User Rights 33
   Managing the Default User Account 34
   Add a User 34
   Assign a Role and Rights to a User 34
   Edit a User Account 34
   Delete a User Account 35

6 Updating System Software 37
   View the Current System Software 37
   Upload an Update 37
   Review the Update History 38

7 Backing Up vShield Manager Data 39
   Back Up Your vShield Manager Data on Demand 39
   Schedule a Backup of vShield Manager Data 40
   Restore a Backup 40

8 System Events and Audit Logs 41
   View the System Event Report 41
   System Event Notifications 42
      vShield Manager Virtual Appliance Events 42
      vShield App Events 42
   Syslog Format 42
   View the Audit Log 43

9 Uninstalling vShield Components 45
   Uninstall a vShield App or vShield Zones 45
   Uninstall a vShield Edge from a Port Group 46
   Uninstall Port Group Isolation from an ESX Host 46
   Uninstall a vShield Endpoint Module 47
      Unregister an SVM from a vShield Endpoint Module 47
      Uninstall the vShield Endpoint Module from the vSphere Client 47

10 vShield Edge Management 49
   View the Status of a vShield Edge 49
   Specify a Remote Syslog Server 50
   Managing the vShield Edge Firewall 50
      Create a vShield Edge Firewall Rule 50
      Validate Active Sessions Against Current vShield Edge Firewall Rules 51
   Manage NAT Rules 51
   Manage DHCP Service 52
   Manage VPN Service 53
   Manage Load Balancer Service 55
   Start or Stop vShield Edge Services 56
   Upgrade vShield Edge Software 56
vShield Edge and Port Group Isolation

vShield App and vShield Endpoint

11 vShield App Management 61
   Send vShield App System Events to a Syslog Server 61
   Back Up the Running CLI Configuration of a vShield App 62
   View the Current System Status of a vShield App 62
   Force a vShield App to Synchronize with the vShield Manager 62
   Restart a vShield App 63
   View Traffic Statistics by vShield App Interface 63

12 Flow Monitoring 65
   Using Flow Monitoring 65
   View a Specific Application in the Flow Monitoring Charts 66
   Change the Date Range of the Flow Monitoring Charts 66
   View the Flow Monitoring Report 66
   Add an App Firewall Rule from the Flow Monitoring Report 67
   Delete All Recorded Flows 68
   Editing Port Mappings 68
      Add an Application-Port Pair Mapping 68
      Delete an Application-Port Pair Mapping 69
      Hide the Port Mappings Table 69

13 App Firewall Management 71
   Using App Firewall 71
      Securing Containers and Designing Security Groups 71
      Default Rules 72
      Layer 4 Rules and Layer 2/Layer 3 Rules 72
      Hierarchy of App Firewall Rules 72
      Planning App Firewall Rule Enforcement 72
   Create an App Firewall Rule 73
   Create a Layer 2/Layer 3 App Firewall Rule 75
   Creating and Protecting Security Groups 75
      Add a Security Group 75
      Assign Resources to a Security Group 76
   Validating Active Sessions against the Current App Firewall Rules 76
   Revert to a Previous App Firewall Configuration 77
   Delete an App Firewall Rule 77
   Using SpoofGuard 77
      SpoofGuard Screen Options 78
      Enable SpoofGuard 78
      Approve IP Addresses 78
      Edit an IP Address 79
      Delete an IP Address 79

14 vShield Endpoint Events and Alarms 81
   View vShield Endpoint Status 81
   Alarms 82
      Host Alarms 82
      SVM Alarms 82
      VM Alarms 83
Appendixes

A Command Line Interface 89
   Logging In and Out of the CLI 89
   CLI Command Modes 89
   CLI Syntax 90
   Moving Around in the CLI 90
   Getting Help within the CLI 91
   Securing CLI User Accounts and the Privileged Mode Password 91
      Add a CLI User Account 91
      Delete the admin User Account from the CLI 92
      Change the CLI Privileged Mode Password 92
   Command Reference 93
      Administrative Commands 93
      CLI Mode Commands 94
      Configuration Commands 97
      Debug Commands 104
      Show Commands 109
      Diagnostics and Troubleshooting Commands 125
      User Administration Commands 128
      Terminal Commands 130
      Deprecated Commands 131

B vShield Edge VPN Configuration Examples 133
   Basic Scenario 133
   Terminology 134
   IKE Phase 1 and Phase 2 134
      Phase 1: Main Mode Transactions 135
      Phase 2: Quick Mode Transactions 135
   Configuring the vShield Edge VPN Parameters 135
   Using a Cisco 2821 Integrated Services Router 137
      Configure Interfaces and Default Route 137
      Configure IKE Policy 137
      Match Each Peer with Its Pre-Shared Secret 138
      Define the IPSEC Transform 138
      Create the IPSEC Access List 138
      Bind the Policy with a Crypto Map and Label It 138
      Bind the Crypto Map to the Outgoing Interface 138
      Example Configuration 138
   Using a Cisco ASA 5510 139
   Using a WatchGuard Firebox X500 141
   Troubleshooting 141
      Successful Negotiation (both Phase 1 and Phase 2) 141
      Phase 1 Policy Not Matching 142
      Phase 2 Not Matching 143
      PFS Mismatch 143
      PSK Not Matching 144
      Packet Capture for a Successful Negotiation 144
C Troubleshooting 149

Troubleshooting vShield Manager Installation 149
  vShield OVA File Extracted to a PC Where vSphere Client Is Not Installed 149
  vShield OVA File Cannot Be Installed in vSphere Client 149
  Cannot Log In to CLI After the vShield Manager Virtual Machine Starts 150
  Cannot Log In to the vShield Manager User Interface 150

Troubleshooting Operation Issues 150
  vShield Manager Cannot Communicate with a vShield App 150
  Cannot Configure a vShield App 150
  Firewall Block Rule Not Blocking Matching Traffic 151
  No Flow Data Displaying in Flow Monitoring 151

Troubleshooting Port Group Isolation Issues 151
  Validate Installation of Port Group Isolation 151
  Verify Install or Uninstall Script 152
  Validate the Data Path 152
  Details of the fence-util Utility 153

Troubleshooting vShield Edge Issues 154
  Virtual Machines Are Not Getting IP Addresses from the DHCP Server 154
  Load-Balancer Does Not Work 154
  Load-Balancer Throws Error 502 Bad Gateway for HTTP Requests 155
  VPN Does Not Work 155

Troubleshooting vShield Endpoint Issues 155
  Thin Agent Logging 155
  Component Version Compatibility 156

Index 157
About This Book

This manual, the vShield Administration Guide, describes how to install, configure, monitor, and maintain the VMware® vShield™ system by using the vShield Manager user interface, the vSphere Client plug-in, and command line interface (CLI). The information includes step-by-step configuration instructions, and suggested best practices.

Intended Audience

This manual is intended for anyone who wants to install or use vShield in a VMware vCenter environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware Infrastructure 4.x, including VMware ESX, vCenter Server, and the vSphere Client.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to http://www.vmware.com/support/pubs.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

vShield Documentation

The following documents comprise the vShield documentation set:
- vShield Administration Guide, this guide
- vShield Quick Start Guide
- vShield API Programming Guide

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.
Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.
vShield Manager and vShield Zones
Overview of vShield

VMware® vShield is a suite of security virtual appliances built for VMware vCenter™ Server and VMware ESX™ integration. vShield is a critical security component for protecting virtualized datacenters from attacks and misuse helping you achieve your compliance-mandated goals.

This guide assumes you have administrator access to the entire vShield system. The viewable resources in the vShield Manager user interface can differ based on the assigned role and rights of a user, and licensing. If you are unable to access a screen or perform a particular task, consult your vShield administrator.

This chapter includes the following topics:
- “vShield Components” on page 13
- “Migration of vShield Components” on page 15
- “VMware Tools” on page 15
- “Ports Required for vShield Communication” on page 15

vShield Components

vShield includes components and services essential for protecting virtual machines. vShield can be configured through a web-based user interface, a vSphere Client plug-in, a command line interface (CLI), and REST API.

To run vShield, you need one vShield Manager virtual machine and at least one vShield App or vShield Edge module.

vShield Manager

The vShield Manager is the centralized network management component of vShield and is installed from OVA as a virtual machine by using the vSphere Client. Using the vShield Manager user interface, administrators install, configure, and maintain vShield components. A vShield Manager can run on a different ESX host from your vShield App and vShield Edge modules.

The vShield Manager leverages the VMware Infrastructure SDK to display a copy of the vSphere Client inventory panel.

For more on the using the vShield Manager user interface, see Chapter 2, “vShield Manager User Interface Basics,” on page 17.

vShield Zones

vShield Zones, included with the vShield Manager, provides firewall protection for traffic between virtual machines. For each Zones Firewall rule, you can specify the source IP, destination IP, source port, destination port, and service.

CAUTION Do not install vShield Zones/App on the ESX host where vCenter Server is running.
vShield Edge

**NOTE** You must obtain an evaluation or full license to use vShield Edge.

vShield Edge provides network edge security and gateway services to isolate the virtual machines in a port group, vDS port group, or Cisco® Nexus 1000V. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, and Load Balancing. Common deployments of vShield Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

**Standard vShield Edge Services (Including Cloud Director)**

- Firewall: Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection for TCP, UDP, and ICMP.
- Network Address Translation: Separate controls for Source and Destination IP addresses, as well as TCP and UDP port translation.
- Dynamic Host Configuration Protocol (DHCP): Configuration of IP pools, gateways, DNS servers, and search domains.

**Advanced vShield Edge Services**

- Site-to-Site Virtual Private Network (VPN): Uses standardized IPsec protocol settings to interoperate with all major firewall vendors.
- Load Balancing: Simple and dynamically configurable virtual IP addresses and server groups.

vShield Edge supports syslog export for all services to remote servers.

vShield App

**NOTE** You must obtain an evaluation or full license to use vShield App.

vShield App is an interior, vNIC-level firewall that allows you to create access control policies regardless of network topology. A vShield App monitors all traffic in and out of an ESX host, including between virtual machines in the same port group. vShield App includes traffic analysis and container-based policy creation.

vShield App installs as a hypervisor module and firewall service virtual appliance. vShield App integrates with ESX hosts through VMsafe APIs and works with VMware vSphere platform features such as DRS, vMotion, DPM, and maintenance mode.

vShield App provides firewalling between virtual machines by placing a firewall filter on every virtual network adapter. The firewall filter operates transparently and does not require network changes or modification of IP addresses to create security zones. You can write access rules by using vCenter containers, like datacenters, cluster, resource pools and vApps, or network objects, like Port Groups and VLANs, to reduce the number of firewall rules and make the rules easier to track.

You should install vShield App instances on all ESX hosts within a cluster so that VMware vMotion™ operations work and virtual machines remain protected as they migrate between ESX hosts. By default, a vShield App virtual appliance cannot be moved by using vMotion.

The Flow Monitoring feature displays allowed and blocked network flows at the application protocol level. You can use this information to audit network traffic and troubleshoot operational.

**CAUTION** Do not install vShield Zones/App on the ESX host where vCenter Server is running.
vShield Endpoint

NOTE You must obtain an evaluation or full license to use vShield Endpoint.

vShield Endpoint delivers an introspection-based antivirus solution. vShield Endpoint uses the hypervisor to scan guest virtual machines from the outside without a bulky agent. vShield Endpoint is efficient in avoiding resource bottlenecks while optimizing memory use.

vShield Endpoint installs as a hypervisor module and security virtual appliance from a third-party antivirus vendor (VMware partners) on an ESX host.

vShield Endpoint provides the following features:
- On-demand file scanning in a service virtual machine.
- On-access file scanning in a service virtual machine.

Migration of vShield Components

The vShield Manager and vShield Edge virtual appliances can be automatically or manually migrated based on DRS and HA policies. The vShield Manager must always be up, so you must migrate the vShield Manager whenever the current ESX host undergoes a reboot or maintenance mode routine.

Each vShield Edge should move with its secured port group to maintain security settings and services.

vShield App and Port Group Isolation services cannot be moved to another ESX host. If the ESX host on which these services reside requires a manual maintenance mode operation, you must de-select the **Move powered off and suspended virtual machines to other hosts in the cluster** check box to ensure these virtual appliances are not migrated. These services restart after the ESX host comes online.

![Confirm Maintenance Mode](image)

VMware Tools

Each vShield virtual appliance includes VMware Tools. Do not upgrade or uninstall the version of VMware Tools included with a vShield virtual appliance.

Ports Required for vShield Communication

The vShield Manager requires the following ports to be open:
- REST API: 80/TCP and 443/TCP
- Graphical User Interface: 80/TCP to 443/TCP and initiates connections to vSphere vCenter SDK.
- SSH access to the CLI (not enabled by default): 22/TCP
The vShield Manager user interface offers configuration and data viewing options specific to vShield use. By utilizing the VMware Infrastructure SDK, the vShield Manager displays your vSphere Client inventory panel for a complete view of your vCenter environment.

**NOTE** You can register the vShield Manager as a vSphere Client plug-in. This allows you to configure vShield components from within the vSphere Client. For more, see “Register the vShield Manager as a vSphere Client Plug-in” on page 22.

The chapter includes the following topics:

- “Logging in to the vShield Manager User Interface” on page 17
- “Accessing the Online Help” on page 18
- “vShield Manager User Interface” on page 18

### Logging in to the vShield Manager User Interface

You access the vShield Manager management interface by using a Web browser.

**To log in to the vShield Manager user interface**

1. Open a Web browser window and type the IP address assigned to the vShield Manager.
   The vShield Manager user interface opens in an SSH session.

2. Accept the security certificate.

   **NOTE** To use an SSL certificate for authentication, see “Add an SSL Certificate to Identify the vShield Manager Web Service” on page 24.

   The vShield Manager login screen appears.

3. Log in to the vShield Manager user interface by using the username **admin** and the password **default**.
   You should change the default password as one of your first tasks to prevent unauthorized use. See “Edit a User Account” on page 34.

4. Click **Log In**.
Accessing the Online Help

The Online Help can be accessed by clicking 🌐 in the upper right of the vShield Manager user interface.

vShield Manager User Interface

The vShield Manager user interface is divided into two panels: the inventory panel and the configuration panel. You select a view and a resource from the inventory panel to open the available details and configuration options in the configuration panel.

When clicked, each inventory object has a specific set of tabs that appear in the configuration panel.

vShield Manager Inventory Panel

The vShield Manager inventory panel hierarchy mimics the vSphere Client inventory hierarchy. Resources include the root folder, datacenters, clusters, port groups, ESX hosts, and virtual machines, including your installed vShield App and vShield Edge modules. As a result, the vShield Manager maintains solidarity with your vCenter Server inventory to present a complete view of your virtual deployment. The vShield Manager is the only virtual machine that does not appear in the vShield Manager inventory panel. vShield Manager settings are configured from the Settings & Reports resource atop the inventory panel.

The inventory panel offers multiple views: Hosts & Clusters, Networks, and Secured Port Groups. The Hosts & Clusters view displays the datacenters, clusters, resource pools, and ESX hosts in your inventory. The Networks view displays the VLAN networks and port groups in your inventory. The Secured Port Groups view displays the port groups protected by vShield Edge instances. The Hosts & Clusters and Networks views are consistent with the same views in the vSphere Client.

There are differences in the icons for virtual machines and vShield components between the vShield Manager and the vSphere Client inventory panels. Custom icons are used to show the difference between vShield components and virtual machines, and the difference between protected and unprotected virtual machines.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>A powered on vShield App in active protection state.</td>
</tr>
<tr>
<td>🌐</td>
<td>A powered off vShield App.</td>
</tr>
<tr>
<td>🌐</td>
<td>A powered on virtual machine that is protected by a vShield App.</td>
</tr>
<tr>
<td>🌐</td>
<td>A powered on virtual machine that is not protected by a vShield App.</td>
</tr>
</tbody>
</table>

Refreshing the Inventory Panel

To refresh the list of resources in the inventory panel, click 🔄. The refresh action requests the latest resource information from the vCenter Server. By default, the vShield Manager requests resource information from the vCenter Server every five minutes.

Searching the Inventory Panel

To search the inventory panel for a specific resource, type a string in the field atop the vShield Manager inventory panel and click 🔍.
vShield Manager Configuration Panel

The vShield Manager configuration panel presents the settings that can be configured based on the selected inventory resource and the output of vShield operation. Each resource offers multiple tabs, each tab presenting information or configuration forms corresponding to the resource.

Because each resource has a different purpose, some tabs are specific to certain resources. Also, some tabs have a second level of options.
Management System Settings

The vShield Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

The chapter includes the following topics:

- “Identify Your vCenter Server” on page 21
- “Register the vShield Manager as a vSphere Client Plug-in” on page 22
- “Identify DNS Services” on page 22
- “Set the vShield Manager Date and Time” on page 23
- “Identify a Proxy Server” on page 23
- “Download a Technical Support Log from a Component” on page 23
- “View vShield Manager System Status” on page 24
- “Add an SSL Certificate to Identify the vShield Manager Web Service” on page 24

Identify Your vCenter Server

After the vShield Manager is installed as a virtual machine, log in to the vShield Manager user interface to connect to your vCenter Server. This enables the vShield Manager to display your VMware Infrastructure inventory.

To identify your vCenter Server from the vShield Manager

1. Log in to the vShield Manager.
   
   Upon initial login, the vShield Manager opens to the Configuration > vCenter tab. If you have previously configured the vCenter tab form, perform the following steps:
   
   a. Click the Settings & Reports from the vShield Manager inventory panel.
   b. Click the Configuration tab.
   
   The vCenter screen appears.

2. Under vCenter Server Information, type the IP address of your vCenter Server in the vSphere Server IP Address/Name field.

3. Type your vSphere Client login user name in the Administrator User Name field.
   
   This user account must have administrator access.
4 Type the password associated with the user name in the **Password** field.
5 Click **Save**.

The vShield Manager connects to the vCenter Server, logs on, and utilizes the VMware Infrastructure SDK to populate the vShield Manager inventory panel. The inventory panel is presented on the left side of the screen. This resource tree should match your VMware Infrastructure inventory panel. The vShield Manager does not appear in the vShield Manager inventory panel.

**Register the vShield Manager as a vSphere Client Plug-in**

The vSphere Plug-in option lets you register the vShield Manager as a vSphere Client plug-in. After the plug-in is registered, you can open the vShield Manager user interface from the vSphere Client.

**To register the vShield Manager as a vSphere Client plug-in**

1 If you are logged in to the vSphere Client, log out.
2 Log in to the vShield Manager.
3 Click **Settings & Reports** from the vShield Manager inventory panel.
4 Click the **Configuration** tab.
   The vCenter screen appears.
5 Under **vSphere Plug-in**, click **Register**.
   Registration might take a few minutes.
6 Log in to the vSphere Client.
7 Select an ESX host.
8 Verify that **vShield Install** appears as a tab.
   You can install and configure vShield components from the vSphere Client.

**Identify DNS Services**

You must specify at least one DNS server during vShield Manager setup. The specified DNS servers appear in the vShield Manager user interface.

In the vShield Manager user interface, you can specify up to three DNS servers that the vShield Manager can use for IP address and host name resolution.

**To identify a DNS server**

1 Click **Settings & Reports** from the vShield Manager inventory panel.
2 Click the **Configuration** tab.
   The vCenter screen appears.
3 Under **DNS Servers**, type an IP address in the **Primary DNS IP Address** to identify the primary DNS server.
   This server is checked first for all resolution requests.
4 (Optional) Type an IP address in the **Secondary DNS IP Address** field.
5 (Optional) Type an IP address in the **Tertiary DNS IP Address** field.
6 Click **Save**.
Set the vShield Manager Date and Time

You can set the date, time, and time zone of the vShield Manager. You can also specify a connection to an NTP server to establish a common network time. Date and time values are used in the system to stamp events as they occur.

To set the date and time configuration of the vShield Manager
1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Configuration tab.
3. Click Date/Time.
4. In the Date and Clock field, type the date and time in the format YYYY-MM-DD HH:MM:SS.
5. In the NTP Server field, type the IP address of your NTP server.
   You can type the hostname of your NTP server if you have set up DNS service.
6. From the Time Zone drop-down menu, select the appropriate time zone.
7. Click Save.

Identify a Proxy Server

If you use a proxy server for network connectivity, you can configure the vShield Manager to use the proxy server. The vShield Manager supports application-level HTTP/HTTPS proxies such as CacheFlow and Microsoft ISA Server.

To identify a proxy server
1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Configuration tab.
3. Click HTTP Proxy.
4. From the Use Proxy drop-down menu, select Yes.
5. (Optional) Type the host name of the proxy server in the Proxy Host Name field.
6. Type the IP address of the proxy server in the Proxy IP Address field.
7. Type the connecting port number on your proxy server in the Proxy Port field.
8. Type the User Name required to log in to the proxy server.
9. Type the Password associated with the user name for proxy server login.
10. Click Save.

Download a Technical Support Log from a Component

You can use the Support option to download the system log from a vShield component to your PC. A system log can be used to troubleshoot operational issues.

To download a vShield component system log
1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Configuration tab.
3. Click Support.
4 Under **Tech Support Log Download**, click **Initiate** next to the appropriate component. Once initiated, the log is generated and uploaded to the vShield Manager. This might take several seconds.

5 After the log is ready, click the **Download** link to download the log to your PC. The log is compressed and has the proprietary file extension .blsl. You can open the log using a decompression utility by browsing for **All Files** in the directory where you saved the file.

**Back Up vShield Manager Data**

You can use the **Backups** option to back up vShield Manager data. See Chapter 7, “Backing Up vShield Manager Data,” on page 39.

**View vShield Manager System Status**

The **Status** tab displays the status of vShield Manager system resource utilization, and includes the software version details, license status, and serial number. The serial number must be registered with technical support for update and support purposes.

**To view the system status of the vShield Manager**

1 Click **Settings & Reports** from the vShield Manager inventory panel.
2 Click the **Configuration** tab.
3 Click **Status**.
4 (Optional) Click **Version Status** to review the current version of system software running on your vShield components.

The **Update Status** tab appears. See “View the Current System Software” on page 37.

**Add an SSL Certificate to Identify the vShield Manager Web Service**

You can generate or import an SSL certificate into the vShield Manager to authenticate the identity of the vShield Manager web service and encrypt information sent to the vShield Manager web server. As a security best practice, you should use the generate certificate option to generate a private key and public key, where the private key is saved to the vShield Manager.

**To generate an SSL certificate**

1 Click **Settings & Reports** from the vShield Manager inventory panel.
2 Click the **Configuration** tab.
3 Click **SSL Certificate**.
4 Under Generate Certificate Signing Request, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>Enter the name that matches the site name. For example, if the IP address of vShield Manager management interface is 192.168.1.10, enter <strong>192.168.1.10</strong>.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Enter the department in your company that is ordering the certificate.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enter the full legal name of your company.</td>
</tr>
<tr>
<td>City Name</td>
<td>Enter the full name of the city in which your company resides.</td>
</tr>
<tr>
<td>State Name</td>
<td>Enter the full name of the state in which your company resides.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Enter the two-digit code that represents your country. For example, the United States is <strong>US</strong>.</td>
</tr>
</tbody>
</table>
To import an SSL certificate

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Configuration tab.
3. Click SSL Certificate.
5. Select the type of certificate file from the Certificate File drop-down list.
6. Click Apply.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Algorithm</td>
<td>Select the cryptographic algorithm to use from either DSA or RSA.</td>
</tr>
<tr>
<td>Key Size</td>
<td>Select the number of bits used in the selected algorithm.</td>
</tr>
</tbody>
</table>
Zones Firewall Management

vShield Zones provides firewall protection access policy enforcement. Traffic details include sources, destinations, direction of sessions, applications, and ports being used. Traffic details can be used to create firewall allow or deny rules.

**NOTE** You can upgrade vShield Zones to vShield App by obtaining a vShield App license. vShield App enhances vShield Zones protection by offering Flow Monitoring, custom container creation (Security Groups), and container-based access policy creation and enforcement.

You do not have to uninstall vShield Zones to install vShield App. All vShield Zones instances become vShield App instances, the Zones Firewall becomes App Firewall, and the additional vShield App features are enabled.

This chapter includes the following topics:

- “Using Zones Firewall” on page 27
- “Create a Zones Firewall Rule” on page 29
- “Create a Layer 2/Layer 3 Zones Firewall Rule” on page 30
- “Validating Active Sessions against the Current Zones Firewall Rules” on page 31
- “Revert to a Previous Zones Firewall Configuration” on page 31
- “Delete a Zones Firewall Rule” on page 32

**Using Zones Firewall**

Zones Firewall is a centralized, hierarchical firewall for ESX hosts. Zones Firewall enables you to create rules that allow or deny access to and from your virtual machines. Each installed vShield Zones enforces the App Zones rules.

You can manage Zones Firewall rules at the datacenter, cluster, and port group levels to provide a consistent set of rules across multiple vShield Zones instances under these containers. As membership in these containers can change dynamically, Zones Firewall maintains the state of existing sessions without requiring reconfiguration of firewall rules. In this way, Zones Firewall effectively has a continuous footprint on each ESX host under the managed containers.

When creating Zones Firewall rules, you create 5-tuple firewall rules based on specific source and destination IP addresses.
Default Rules

By default, Zones Firewall enforces a set of rules allowing traffic to pass through all vShield Zones instances. These rules appear in the Default Rules section of the Zones Firewall table. The default rules cannot be deleted or added to. However, you can change the Action element of each rule from Allow to Deny.

Layer 4 Rules and Layer 2/Layer 3 Rules

Zones Firewall offers two sets of configurable rules: L4 (Layer 4) rules and L2/L3 (Layer 2/Layer 3) rules. Layers refer to layers of the Open Systems Interconnection (OSI) Reference Model.

Layer 4 rules govern TCP and UDP transport of Layer 7, or application-specific traffic. Layer 2/Layer 3 rules monitor traffic from ICMP, ARP, and other Layer 2 and Layer 3 protocols. You can configure Layer 2/Layer 3 rules at the datacenter level only. By default, all Layer4 and Layer 2/Layer 3 traffic is allowed to pass.

Hierarchy of Zones Firewall Rules

Each vShield Zones instance enforces Zones Firewall rules in top-to-bottom ordering. A vShield Zones instance checks each traffic session against the top rule in the Zones Firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced.

Zones Firewall rules are enforced in the following hierarchy:

1. Data Center High Precedence Rules
2. Cluster Level Rules
3. Data Center Low Precedence Rules (see Rules below this level have lower precedence than cluster level rules when a datacenter resource is selected)
4. Secure Port Group Rules
5. Default Rules

Zones Firewall offers container-level and custom priority precedence configurations:

- Container-level precedence refers to recognizing the datacenter level as being higher in priority than the cluster level. When a rule is configured at the datacenter level, the rule is inherited by all clusters and vShield agents therein. A cluster-level rule is only applied to the vShield Zones instances within the cluster.

- Custom priority precedence refers to the option of assigning high or low precedence to rules at the datacenter level. High precedence rules work as noted in the container-level precedence description. Low precedence rules include the Default Rules and the configuration of Data Center Low Precedence rules. This flexibility allows you to recognize multiple layers of applied precedence.

At the cluster level, you configure rules that apply to all vShield Zones instances within the cluster. Because Data Center High Precedence Rules are above Cluster Level Rules, ensure your Cluster Level Rules are not in conflict with Data Center High Precedence Rules.

Planning Zones Firewall Rule Enforcement

Using Zones Firewall, you can configure allow and deny rules based on your network policy. The following examples represent two common firewall policies:

- Allow all traffic by default. You keep the default allow all rules and add deny rules based on Flow Monitoring data or manual App Firewall configuration. In this scenario, if a session does not match any of the deny rules, the vShield App allows the traffic to pass.

- Deny all traffic by default. You can change the Action status of the default rules from Allow to Deny, and add allow rules explicitly for specific systems and applications. In this scenario, if a session does not match any of the allow rules, the vShield App drops the session before it reaches its destination. If you change all of the default rules to deny any traffic, the vShield App drops all incoming and outgoing traffic.
Create a Zones Firewall Rule

Zones Firewall rules allow or deny traffic based on the following criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source (A.B.C.D/nn)</td>
<td>IP address with netmask (nn) from which the communication originated</td>
</tr>
<tr>
<td>Source Port</td>
<td>Port or range of ports from which the communication originated. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.</td>
</tr>
<tr>
<td>Destination (A.B.C.D/nn)</td>
<td>IP address with netmask (nn) which the communication is targeting</td>
</tr>
<tr>
<td>Destination Application</td>
<td>The application on the destination the source is targeting</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port or range of ports which the communication is targeting. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol used for communication</td>
</tr>
</tbody>
</table>

You can add destination and source port ranges to a rule for dynamic services such as FTP and RPC, which require multiple ports to complete a transmission. If you do not allow all of the ports that must be opened for a transmission, the transmission fails.

**To create a firewall rule at the datacenter level**

1. In the vSphere Client, go to Inventory > Hosts and Clusters.
2. Select a datacenter resource from the resource tree.
3. Click the vShield Zones tab.
4. Click Zones Firewall.
   - By default, the L4 Rules option is selected.
   - To create L2/L3 rules, see “Create a Layer 2/Layer 3 Zones Firewall Rule” on page 30.
5. Do one of the following:
   - Click Add to add a new rule to the Data Center Low Precedence Rules (Rules below this level have lower precedence...).
   - Select a row in the Data Center High Precedence Rules section of the table and click Add. A new row appears below the selected row.
6. Double-click each cell in the new row to select the appropriate information.
   - You must type IP addresses in the Source and Destination fields, and port numbers in the Source Port and Destination Port fields.
7. (Optional) Select the new row and click Up to move the row up in priority.
8. (Optional) Select the Log check box to log all sessions matching this rule.
9. Click Commit to save the rule.

**To create a firewall rule at the cluster level**

1. In the vSphere Client, go to Inventory > Hosts and Clusters.
2. Select a cluster resource from the resource tree.
3. Click the vShield Zones tab.
4. Click Zones Firewall.
   - By default, the L4 Rules option is selected.
   - To create L2/L3 rules, see “Create a Layer 2/Layer 3 Zones Firewall Rule” on page 30.
Click Add.
A new row appears in the Cluster Level Rules section of the table.
Double-click each cell in the new row to select the appropriate information.
You must type IP addresses in the Source and Destination fields, and port numbers in the Source Port and Destination Port fields.
(Optional) Select the new row and click Up to move the row up in priority.
(Optional) Select the Log check box to log all sessions matching this rule.
Click Commit to save the rule.

To create a firewall rule at the port group level
1 In the vSphere Client, go to Inventory > Networking.
2 Select a port group from the resource tree.
3 Click the vShield Zones tab.
4 Click Zones Firewall.
5 Click Add.
A new row is added at the bottom of the Secure Port Group Rules section.
Double-click each cell in the new row to select the appropriate information.
You must type IP addresses in the Source and Destination fields, and port numbers in the Source Port and Destination Port fields.
(Optional) Select the new row and click Up to move the row up in priority.
(Optional) Select the Log check box to log all sessions matching this rule.
Click Commit to save the rule.

Create a Layer 2/Layer 3 Zones Firewall Rule
The Layer 2/Layer 3 firewall enables configuration of allow or deny rules for common Data Link Layer and Network Layer requests, such as ICMP pings and traceroutes.
You can change the default Layer 2/Layer 3 rules from allow to deny based on your network security policy.
Layer 4 firewall rules allow or deny traffic based on the following criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source (A.B.C.D/nn)</td>
<td>IP address with netmask (nn) from which the communication originated</td>
</tr>
<tr>
<td>Destination (A.B.C.D/nn)</td>
<td>IP address with netmask (nn) which the communication is targeting</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol used for communication</td>
</tr>
</tbody>
</table>

To create a Layer 2/Layer 3 firewall rule
1 In the vSphere Client, go to Inventory > Hosts and Clusters.
2 Select a datacenter resource from the resource tree.
3 Click the vShield Zones tab.
4 Click Zones Firewall.
5 Click L2/L3 Rules.
6 Click Add.
A new row is added at the bottom of the DataCenter Rules section of the table.
7 Double-click each cell in the new row to type or select the appropriate information.
   You can type IP addresses in the Source and Destination fields

8 (Optional) Select the Log check box to log all sessions matching this rule.

9 Click Commit.

Validating Active Sessions against the Current Zones Firewall Rules

By default, a vShield Zones instance matches firewall rules against each new session. After a session has been established, any firewall rule changes do not affect active sessions.

The CLI command validate sessions enables you to validate active sessions against the current Zones Firewall rule set to purge any sessions that are in violation of the current rule set. After a firewall rule set update, you should validate active sessions to purge any existing sessions that are in violation of the updated policy.

After the Zones Firewall update is complete, issue the validate sessions command from the CLI of a vShield Zones instance to purge sessions that are in violation of current policy.

To validate active sessions against the current firewall rules

1 Update and commit the Zones Firewall rule set at the appropriate container level.

2 Open a console session on a vShield Zones instance issue the validate sessions command.

   vShieldZones> enable
   Password:
   vShieldZones# validate sessions

Revert to a Previous Zones Firewall Configuration

The vShield Manager saves a snapshot of App Firewall settings each time you commit a new rule. Clicking Commit causes the vShield Manager to save the previous configuration with a timestamp before adding the new rule. These snapshots are available from the Revert to Snapshot drop-down menu.

To revert to a previous App Firewall configuration

1 In the vSphere Client, go to Inventory > Hosts and Clusters.

2 Select a datacenter or cluster resource from the inventory panel.

3 Click the vShield Zones tab.

4 Click Zones Firewall.

5 From the Revert to Snapshot drop-down list, select a snapshot.
   Snapshots are presented in the order of timestamps, with the most recent snapshot listed at the top.

6 View snapshot configuration details.

7 Do one of the following:
   - To return to the current configuration, select the - option from the Revert to Snapshot drop-down list.
   - Click Commit to overwrite the current configuration with the snapshot configuration.
Delete a Zones Firewall Rule

You can delete any App Firewall rule you have created. You cannot delete the any rules in the Default Rules section of the table.

To delete an App Firewall rule

1 Click an existing row in the Zones Firewall table.
2 Click Delete.
3 Click Commit.
Security operations are often managed by multiple individuals. Management of the overall system is delegated to different personnel according to some logical categorization. However, permission to carry out tasks is limited only to users with appropriate rights to specific resources. From the Users section, you can delegate such resource management to users by granting applicable rights.

User management in the vShield Manager user interface is separate from user management in the CLI of any vShield component.

This chapter includes the following topics:

- “Managing User Rights” on page 33
- “Add a User” on page 34
- “Assign a Role and Rights to a User” on page 34
- “Edit a User Account” on page 34
- “Delete a User Account” on page 35

Managing User Rights

Within the vShield Manager user interface, a user’s rights define the actions the user is allowed to perform on a given resource. Rights determine the user’s authorized activities on the given resource, ensuring that a user has access only to the functions necessary to complete applicable operations. This allows domain control over specific resources, or system-wide control if your right encompasses the System resource.

The following rules are enforced:

- A user can only have one right to one resource.
- A user cannot add to or remove assigned rights and resources.

Table 5-1. vShield Manager User Rights

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Read only</td>
</tr>
<tr>
<td>CRUD</td>
<td>Read and Write</td>
</tr>
</tbody>
</table>

Table 5-2. vShield Manager User Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Access to entire vShield system</td>
</tr>
<tr>
<td>Datacenter</td>
<td>Access to a specified datacenter resource</td>
</tr>
<tr>
<td>Cluster</td>
<td>Access to a specified cluster resource</td>
</tr>
<tr>
<td>None</td>
<td>Access to no resources</td>
</tr>
</tbody>
</table>
Managing the Default User Account

The vShield Manager user interface includes one default user account, user name admin, which has rights to all resources. You cannot edit the rights of or delete this user. The default password for admin is default.

Change the password for this account upon initial login to the vShield Manager. See “Edit a User Account” on page 34.

Add a User

Basic user account creation requires assigning the user a login name and password.

To create a new user account

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Users tab.
3. Click Create User.
   The New User screen opens.
4. Type a User Name.
   This is used for login to the vShield Manager user interface. This user name and associated password cannot be used to access the vShield App or vShield Manager CLIs.
5. (Optional) Type the user’s Full Name for identification purposes.
6. (Optional) Type an Email Address.
7. Type a Password for login.
8. Re-type the password in the Retype Password field.
9. Click OK.

   After account creation, you configure right and resource assignment separately.

Assign a Role and Rights to a User

After creating a user account, you can assign the user a role and rights to system resources. The role defines the resource, and the right defines the user’s access to that resource.

To assign a role and right to a user

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Users tab.
3. Double-click the Resource cell for the user.
4. From the drop-down menu that opens, select an available resource.
5. Double-click the Access Right cell for the user.
6. From the drop-down menu that opens, select an available access right.

Edit a User Account

You can edit a user account to change the password.

To edit an existing user account

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Users tab.
3. Click a cell in the table row that identifies the user account.
4 Click **Update User**.

5 Make changes as necessary.
   If you are changing the password, confirm the password by typing it a second time in the **Retype Password** field.

6 Click **OK** to save your changes.

**Delete a User Account**

You can delete any created user account. You cannot delete the **admin** account. Audit records for deleted users are maintained in the database and can be referenced in an Audit Log report.

**To delete a user account**

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Users** tab.

3 Click a cell in the table row that identifies the user account.

4 Click **Delete User**.
Updating System Software

vShield software requires periodic updates to maintain system performance. Using the Updates tab options, you can install and track system updates.

This chapter includes the following topics:

- “View the Current System Software” on page 37
- “Upload an Update” on page 37
- “Review the Update History” on page 38

View the Current System Software

The current versions of vShield component software display under the Update Status tab.

To view the current system software

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Updates tab.
3. Click Update Status.

Upload an Update

vShield updates are available as offline updates. When an update is made available, you can download the update to your PC, and then upload the update by using the vShield Manager user interface.

When the update is uploaded, the vShield Manager is updated first, after which, each vShield App is updated. If a reboot of either the vShield Manager or a vShield App is required, the Update Status screen prompts you to reboot the component. In the event that both the vShield Manager and all vShield App instances must be rebooted, you must reboot the vShield Manager first, and then reboot each vShield App.

To upload an update

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Updates tab.
3. Click Upload Settings.
4. Click Browse to locate the update.
5. After locating the file, click Upload File.
6 Click **Confirm Install** to confirm update installation.

There are two tables on this screen. During installation, you can view the top table for the description, start time, success state, and process state of the current update. View the bottom table for the update status of each vShield App. All vShield App instances have been upgraded when the status of the last vShield App is displayed as **Finished**.

7 After the vShield Manager reboots, click the **Update Status** tab.

8 Click **Reboot Manager** if prompted.

9 Click **Finish Install** to complete the system update.

10 Click **Confirm**.

**Review the Update History**

The **Update History** tab lists the updates that have already been installed, including the installation date and a brief description of each update.

**To view a history of installed updates**

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Updates** tab.

3 Click **Update History**.
Back Up vShield Manager Data

You can back up and restore your vShield Manager data, which can include system configuration, events, and audit log tables. Configuration tables are included in every backup. You can, however, exclude system and audit log events. Backups are saved to a remote location that must be accessible by the vShield Manager.

Backups can be executed according to a schedule or on demand.

This chapter includes the following topics:

- “Back Up Your vShield Manager Data on Demand” on page 39
- “Schedule a Backup of vShield Manager Data” on page 40
- “Restore a Backup” on page 40

Back Up Your vShield Manager Data on Demand

You can back up vShield Manager data at any time by performing an on-demand backup.

To back up the vShield Manager database

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Configuration tab.
3. Click Backups.
4. (Optional) Select the Exclude System Events check box if you do not want to back up system event tables.
5. (Optional) Select the Exclude Audit Logs check box if you do not want to back up audit log tables.
6. Type the Host IP Address of the system where the backup will be saved.
7. (Optional) Type the Host Name of the backup system.
8. Type the User Name required to log in to the backup system.
9. Type the Password associated with the user name for the backup system.
10. In the Backup Directory field, type the absolute path where backups are to be stored.
11. Type a text string in Filename Prefix.
   - This text is prepended to the backup filename for easy recognition on the backup system. For example, if you type ppdb, the resulting backup is named as ppdbHH_MM_SS_DayDDMonYYYY.
12. From the Transfer Protocol drop-down menu, select either SFTP or FTP.
13. Click Backup.
   - Once complete, the backup appears in a table below this form.
14. Click Save Settings to save the configuration.
Schedule a Backup of vShield Manager Data

You can only schedule the parameters for one type of backup at any given time. You cannot schedule a configuration-only backup and a complete data backup to run simultaneously.

To schedule periodic backups of your vShield Manager data

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Configuration tab.
3. Click Backups.
4. From the Scheduled Backups drop-down menu, select On.
5. From the Backup Frequency drop-down menu, select Hourly, Daily, or Weekly.
   The Day of Week, Hour of Day, and Minute drop-down menus are disabled based on the selected frequency. For example, if you select Daily, the Day of Week drop-down menu is disabled as this field is not applicable to a daily frequency.
6. (Optional) Select the Exclude System Events check box if you do not want to back up system event tables.
7. (Optional) Select the Exclude Audit Log check box if you do not want to back up audit log tables.
8. Type the Host IP Address of the system where the backup will be saved.
9. (Optional) Type the Host Name of the backup system.
10. Type the User Name required to login to the backup system.
11. Type the Password associated with the user name for the backup system.
12. In the Backup Directory field, type the absolute path where backups will be stored.
13. Type a text string in Filename Prefix.
   This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type `ppdb`, the resulting backup is named as `ppdbHH_MM_SS_DayDDMonYYYY`.
14. From the Transfer Protocol drop-down menu, select either SFTP or FTP, based on what the destination supports.
15. Click Save Settings.

Restore a Backup

To restore an available backup, the Host IP Address, User Name, Password, and Backup Directory fields in the Backups screen must have values that identify the location of the backup to be restored. When you restore a backup, the current configuration is overridden. If the backup file contains system event and audit log data, that data is also restored.

IMPORTANT Back up your current data before restoring a backup file.

To restore an available vShield Manager backup

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Configuration tab.
3. Click Backups.
4. Click View Backups to view all available backups saved to the backup server.
5. Select the check box for the backup to restore.
6. Click Restore.
7. Click OK to confirm.
System Events and Audit Logs

System events are events that are related to vShield operation. They are raised to detail every operational event, such as a vShield App reboot or a break in communication between a vShield App and the vShield Manager. Events might relate to basic operation (Informational) or to a critical error (Critical).

This chapter includes the following topics:

- “View the System Event Report” on page 41
- “System Event Notifications” on page 42
- “Syslog Format” on page 42
- “View the Audit Log” on page 43

View the System Event Report

The vShield Manager aggregates system events into a static report.

To view the System Event report

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the System Events tab.
System Event Notifications

vShield Manager Virtual Appliance Events

<table>
<thead>
<tr>
<th>Power Off</th>
<th>Power On</th>
<th>Interface Down</th>
<th>Interface Up</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local CLI</strong></td>
<td>Run show log follow command.</td>
<td>Run show log follow command.</td>
<td>Run show log follow command.</td>
</tr>
<tr>
<td><strong>GUI</strong></td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local CLI</strong></td>
<td>Run show process monitor command.</td>
<td>Run show system memory command.</td>
</tr>
<tr>
<td><strong>GUI</strong></td>
<td>See “View vShield Manager System Status” on page 24.</td>
<td>See “View vShield Manager System Status” on page 24.</td>
</tr>
</tbody>
</table>

vShield App Events

<table>
<thead>
<tr>
<th>Power Off</th>
<th>Power On</th>
<th>Interface Down</th>
<th>Interface Up</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local CLI</strong></td>
<td>Run show log follow command.</td>
<td>Run show log follow command.</td>
<td>Run show log follow command.</td>
</tr>
<tr>
<td><strong>Syslog</strong></td>
<td>NA</td>
<td>e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex. For scripting on the syslog server, search for NIC Link is.</td>
<td>e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex. For scripting on the syslog server, search for NIC Link is.</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td>Memory</td>
<td>Storage</td>
<td>Session reset due to DoS, inactivity, or data timeouts</td>
</tr>
<tr>
<td><strong>Local CLI</strong></td>
<td>Run show process monitor command.</td>
<td>Run show system memory command.</td>
<td>Run show filesystem command.</td>
</tr>
<tr>
<td><strong>Syslog</strong></td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Syslog Format

The system event message logged in the syslog has the following structure:

- syslog header (timestamp + hostname + sysmgr/)
- Timestamp (from the service)
- Name/value pairs
  - Name and value separated by delimiter '::' (double colons)
  - Each name/value pair separated by delimiter ';;' (double semi-colons)
The fields and types of the system event are:

- Event ID :: 32 bit unsigned integer
- Timestamp :: 32 bit unsigned integer
- Application Name :: string
- Application Submodule :: string
- Application Profile :: string
- Event Code :: integer (possible values: 10007 10016 10043 20019)
- Severity :: string (possible values: INFORMATION LOW MEDIUM HIGH CRITICAL)
- Message ::

View the Audit Log

The Audit Logs tab provides a view into the actions performed by all vShield Manager users. The vShield Manager retains audit log data for one year, after which time the data is discarded.

To view the Audit Log

1. Click Settings & Reports from the vShield Manager inventory panel.
2. Click the Audit Logs tab.
3. Narrow the output by clicking one or more of the following column filters:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Select the login name of a user who performed the action.</td>
</tr>
<tr>
<td>Module</td>
<td>Select the vShield resource on which the action was performed.</td>
</tr>
<tr>
<td>Operation</td>
<td>Select the type of action performed.</td>
</tr>
<tr>
<td>Status</td>
<td>Select the result of action as either Success or Failure.</td>
</tr>
<tr>
<td>Operation Span</td>
<td>Select the vShield component on which the action was performed. Local refers to the vShield Manager.</td>
</tr>
</tbody>
</table>
Uninstalling vShield Components

This chapter details the steps required to uninstall vShield components from your vCenter inventory.

This chapter includes the following topics:

- “Uninstall a vShield App or vShield Zones” on page 45
- “Uninstall a vShield Edge from a Port Group” on page 46
- “Uninstall Port Group Isolation from an ESX Host” on page 46
- “Uninstall a vShield Endpoint Module” on page 47

**NOTE** The vShield Quick Start Guide details installation of vShield components.

Uninstall a vShield App or vShield Zones

Uninstalling a vShield App or vShield Zones removes the agent from the network.

**CAUTION** Uninstalling a vShield App or vShield Zones places the ESX host in maintenance mode. After uninstallation is complete, the ESX host reboots. If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue. If the vShield Manager is on the same ESX host, the vShield Manager must be migrated prior to uninstalling the vShield App or vShield Zones.

To uninstall a vShield App or vShield Zones instance

1. Log in to the vSphere Client.
2. Select the ESX host from the inventory tree.
3. Click the vShield tab.
4. Click **Uninstall** for the vShield App or vShield Zones service.

   The instance is uninstalled.
Uninstall a vShield Edge from a Port Group

You can uninstall a vShield Edge from a port group by using the vSphere Client.

**CAUTION** If you have enabled Port Group Isolation, you must migrate or power off the virtual machines on the ESX host from which you want to uninstall a vShield Edge. Uninstalling Port Group Isolation places the ESX host in maintenance mode. After uninstallation is complete, the ESX host reboots. If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue. If the vShield Manager is on the same ESX host, the vShield Manager must be migrated prior to uninstalling Port Group Isolation.

If you did not install and enable Port Group Isolation on an ESX host, you do not have to migrate virtual machines to uninstall a vShield Edge.

**To uninstall a vShield Edge**

1. Log in to the vSphere Client.
2. Go to View > Inventory > Networking.
3. Click the Edge tab.
4. Click Uninstall.

Uninstall Port Group Isolation from an ESX Host

Uninstalling Port Group Isolation requires multiple steps that must be performed in the following order.

**CAUTION** Uninstalling Port Group Isolation places the ESX host in maintenance mode. After uninstallation is complete, the ESX host reboots. If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue. If the vShield Manager is on the same ESX host, the vShield Manager must be migrated prior to uninstalling Port Group Isolation.

**To uninstall Port Group Isolation**

1. Migrate all vShield Edge instances and their secured port groups off the ESX host from which Port Group Isolation is being uninstalled.
2. Go to View > Inventory > Networking.
3. Right-click the vDS from which Port Group Isolation will be uninstalled.
4. Select vShield > Disable Isolation.
5. Go to View > Inventory > Hosts and Clusters.
6. Click the ESX host from the vSphere Client inventory panel on which Port Group Isolation is installed.
7. Click the vShield tab.
8. Click Uninstall for the vShield Edge Port Group Isolation service.
Uninstall a vShield Endpoint Module

Before you uninstall the vShield Endpoint module from the vShield Manager, you must unregister the SVM from the vShield Endpoint module.

**CAUTION** Uninstalling vShield Endpoint places the ESX host in maintenance mode. After uninstallation is complete, the ESX host reboots. If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue. If the vShield Manager is on the same ESX host, the vShield Manager must be migrated prior to uninstalling vShield Endpoint.

Unregister an SVM from a vShield Endpoint Module

You must specify the virtual machine ID of the SVM to unregister the SVM from the vShield Endpoint module.

**Example 9-1. Unregistering an SVM**

Request:

DELETE <vshieldmanager-uri>/endpointsecurity/svm/<vmId>

Example:

DELETE /api/1.0/endpointsecurity/svm/vm-1234 HTTP/1.1
host: 10.112.199.123:80
Authorization: Basic YWRtaW46ZGVmYXVsdA==

Response:

HTTP 204 No Content: The Endpoint Security VM is successfully unregistered.
HTTP 401 Unauthorized: The username or password sent in Authorized header is wrong.
HTTP 405 Method Not Allowed: If the vmId is missed in the URI.
HTTP 400 Bad Request: Internal error codes. Please refer the Error Schema for more details.
  40002=Acquiring data from VC failed for <>
  40007=SVM with moid: <> not registered
  40015=vmId is malformatted or of incorrect length : <>

Uninstall the vShield Endpoint Module from the vSphere Client

Uninstalling an vShield Endpoint module puts the ESX host into maintenance mode and reboots it.

**CAUTION** Migrate your vShield Manager and any other virtual machines to another ESX host to avoid shutting down these virtual machines during reboot.

To uninstall an vShield Endpoint module from an ESX host

1. Log in to the vSphere Client.
2. Select an ESX host from the inventory tree.
3. Click the vShield tab.
4. Click Uninstall for to the vShield Endpoint service.

Uninstallation removes port group epsec-vmk-1 and vSwitch epsec-vswitch-2.
vShield Edge provides network edge security and gateway services to isolate the virtual machines in a port group, vDS port group, or Cisco® Nexus 1000V. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, and Load Balancing. Common deployments of vShield Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

This chapter includes the following topics:

- “View the Status of a vShield Edge” on page 49
- “Specify a Remote Syslog Server” on page 50
- “Managing the vShield Edge Firewall” on page 50
- “Manage NAT Rules” on page 51
- “Manage DHCP Service” on page 52
- “Manage VPN Service” on page 53
- “Manage Load Balancer Service” on page 55
- “Start or Stop vShield Edge Services” on page 56
- “Upgrade vShield Edge Software” on page 56

View the Status of a vShield Edge

The Status option presents the network configuration and status of services of a vShield Edge module. Details include interface addressing and network ID. You can use the network ID to send REST API commands to a vShield Edge module.

To view the status of a vShield App

1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the Edge tab.
4. Click the Status link.
Specify a Remote Syslog Server

You can send vShield Edge events, such as violated firewall rules, to a syslog server.

To specify a remote syslog server
1 In the vSphere Client, go to Inventory > Networking.
2 Select an internal port group that is protected by a vShield Edge.
3 Click the vShield Edge tab.
4 Click the Status link.
5 Under Remote Syslog Servers, place the cursor in the top text box and type the IP address of a remote syslog server.
6 Click Commit to save the configuration.

Managing the vShield Edge Firewall

The vShield Edge provides firewall protection for incoming and outgoing sessions. The default firewall policy allows all traffic to pass. In addition to the default firewall policy, you can configure a set of rules to allow or deny traffic sessions to and from specific sources and destinations. You manage the default firewall policy and firewall rule set separately for each vShield Edge agent.

You can change the Default Policy from Allow to Deny on a vShield Edge to deny any sessions that do not match any of the current firewall rules.

Create a vShield Edge Firewall Rule

vShield Edge firewall rules police traffic based on the following criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>IP address from which the communication originated.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Port or range of ports from which the communication originated. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>IP address which the communication is targeting.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port or range of ports which the communication is targeting. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol used for communication.</td>
</tr>
<tr>
<td>Direction</td>
<td>Direction of transmission. Options are IN, OUT, or BOTH.</td>
</tr>
<tr>
<td>Action</td>
<td>Action to enforce on transmission. Options are ALLOW or DENY. The default action on all traffic is ALLOW.</td>
</tr>
</tbody>
</table>

You can add destination and source port ranges to a rule for dynamic services such as FTP and RPC, which require multiple ports to complete a transmission. If you do not allow all of the ports that must be opened for a transmission, the transmission is blocked.

To create a vShield Edge firewall rule
1 In the vSphere Client, go to Inventory > Networking.
2 Select an internal port group that is protected by a vShield Edge.
3 Click the vShield Edge tab.
4 Click the Firewall link.
5 Click **Add**.
A new row appears in the table.

6 Double-click each cell in the row to enter or select the appropriate information.
You must type IP addresses in the **Source** and **Destination** fields.

7 (Optional) Click **Log** to send log events to a specified syslog server when the firewall rule is violated.

8 (Optional) Select the new row and click **Move Up** to move the rule up in priority.

9 Click **Commit** to save the rule.

**Validate Active Sessions Against Current vShield Edge Firewall Rules**

By default, a vShield Edge matches firewall rules against each new session. After a session has been established, any firewall rule changes do not affect active sessions.

The CLI command **validate sessions** enables you to validate active sessions against the current vShield Edge firewall rule set to purge any sessions that are in violation of the current rule set. After a firewall rule set update, you should validate active sessions to purge any existing sessions that are in violation of the updated policy.

After a vShield Edge firewall update is complete, issue the **validate sessions** command from the CLI of a vShield Edge instance to purge sessions that are in violation of current policy.

**To validate active sessions against the current firewall rules**

1 Update and commit the vShield Edge firewall rule set.
2 Open a console session on a vShield Edge instance to issue the **validate sessions** command.
   ```
   vShieldEdge> validate sessions
   ```

**Manage NAT Rules**

The vShield Edge provides network address translation (NAT) service to protect the IP addresses of internal, private networks from the public network. You must configure NAT rules to provide access to services running on privately addressed virtual machines.

The NAT service configuration is separated into SNAT and DNAT rules. An SNAT rule translates a private internal IP address into a public IP address for outbound traffic. A DNAT rule maps a public IP address to a private internal IP address.

**To configure an SNAT rule for a vShield Edge**

1 In to the vSphere Client, go to **Inventory** > **Networking**.
2 Select an Internal port group where a vShield Edge has been installed.
3 Click the **vShield Edge** tab.
4 Click the **NAT** link.
5 Under Direction OUT (SNAT), click **Add**.
   A new row appears in the table.
6 Double-click each cell in the row to enter the appropriate information.
7 Click **Commit** to save the rule.
To configure a DNAT rule for a vShield Edge
1. In the vSphere Client, go to Inventory > Networking.
2. Select an Internal port group where a vShield Edge has been installed.
3. Click the vShield Edge tab.
4. Click the NAT link.
5. Under Direction In (DNAT), click Add.
   A new row appears in the table.
6. Double-click each cell in the row to enter or select the appropriate information.
7. Click Commit to save the rule.

Manage DHCP Service
vShield Edge supports IP address pooling and one-to-one static IP address allocation. Static IP address binding is based on the vCenter managed object ID and interface ID of the requesting client.

vShield Edge DHCP service adheres to the following rules:
- Listens on the vShield Edge internal interface for DHCP discovery.
- Uses the IP address of the internal interface on the vShield Edge as the default gateway address for all clients, and the broadcast and subnet mask values of the internal interface for the container network.

To add a DHCP IP pool
1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the vShield Edge tab.
4. Click the DHCP link.
   A new row appears in the table.
6. Double-click each cell in the row to enter or select the appropriate information.
   The Primary Name Server and Secondary Name Server fields refer to DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
7. Click Commit to save the rule.
8. If DHCP service has not been enabled, enable DHCP service.
   See “Start or Stop vShield Edge Services” on page 56.

To add a DHCP static binding
1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the vShield Edge tab.
4. Click the DHCP link.
5 Under Static Bindings, click Add Bindings.
A new row appears in the table.

6 Double-click each cell in the row to enter or select the appropriate information.
The Primary Name Server and Secondary Name Server fields refer to DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.

7 Click Commit to save the rule.

8 If DHCP service has not been enabled, enable DHCP service.
See “Start or Stop vShield Edge Services” on page 56.

Manage VPN Service

vShield Edge modules support site-to-site IPSec VPN between a vShield Edge and remote sites.

Figure 10-1. vShield Edge Providing VPN Access from a Remote Site to a Secured Port Group

At this time, vShield Edge supports pre-shared key mode, IP unicast traffic, and no dynamic routing protocol between the vShield Edge and remote VPN routers. Behind each remote VPN router, you can configure multiple subnets to connect to the internal network behind a vShield Edge through IPSec tunnels. These subnets and the internal network behind a vShield Edge must have non-overlapping address ranges.

You can deploy a vShield Edge agent behind a NAT device. In this deployment, the NAT device translates the VPN address of a vShield Edge into a publicly accessible address facing the Internet. Remote VPN routers use this public address to access the vShield Edge.

Remote VPN routers can be located behind a NAT device as well. You must provide both the VPN native address and the NAT public address to set up the tunnel.

On both ends, static one-to-one NAT is required for the VPN address.
To configure VPN on a vShield Edge
1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the vShield Edge tab.
4. Click the VPN link.
5. Type an External IP Address for the VPN service on the vShield Edge.
6. Type the NATed Public IP that represents the External IP Address to the external network.
7. Select the Log check box to log VPN activity.
8. Click Apply.
   Next, identify a peer site.

To identify a VPN peer site
1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the vShield Edge tab.
4. Click the VPN link.
5. Under Peer Site Configuration, click Create Site.
6. Type a name to identify the site in Site Name.
7. Type the IP address of the site in Remote EndPoint.
8. Type the Shared Secret.
9. Type an MTU threshold.
10. Click Add.
    Next, add a tunnel to connect to the site.

To identify a VPN peer site
1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the vShield Edge tab.
4. Click the VPN link.
5. Under Peer Site Configuration, select the appropriate peer from the Select or create a site drop-down list.
6. Click Add Tunnel.
7. Double-click the Tunnel Name cell and type a name to identify the tunnel.
8. Double-click the Remote Site Subnet cell and enter the IP address in CIDR format (A.B.C.D/M).
9. Double-click the Encryption cell and select the appropriate encryption type.
10. Click Commit.
11. Enable VPN service. See “Start or Stop vShield Edge Services” on page 56.
Manage Load Balancer Service

The vShield Edge provides load balancing for HTTP traffic. Load balancing (up to Layer 7) enables Web application auto-scaling.

**Figure 10-2.** vShield Edge Providing Load Balancing Service for Protected Virtual Machines

You map an external (or public) IP address to a set of internal servers for load balancing. The load balancer accepts HTTP requests on the external IP address and decides which internal server to use. Port 80 is the default listening port for load balancer service.

**To configure load balancer service**

1. In the vSphere Client, go to **Inventory > Networking**.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the **vShield Edge** tab.
4. Click the **Load Balancer** link.
5. Click **Add Rule** above the External IP Addresses table.

   A new row appears in the table.
6. Double-click the External IP Addresses column cell to enter the external IP address.
7. Double-click the Algorithm column cell to select the routing algorithm.
8. (Optional) Select the Logging check box to send a syslog event for each request to the external IP address.
9. Press **ENTER**.
10. Click **Add Rule** above the Load Balanced Servers IP Addresses table.
11. Double-click the cell to enter the IP address of the first web server.
12. Press **ENTER**.
13. Click **Add Rule** above the Load Balanced Servers IP Addresses table.
14. Double-click the new cell to enter the IP address of the second web server.
15 Press ENTER. You can add additional web servers in the same manner.

16 Click Commit.

17 If load balancer service has not been enabled, enable the service. See “Start or Stop vShield Edge Services” on page 56.

Start or Stop vShield Edge Services

You can start and stop the VPN, DHCP, and load balancing services of a vShield Edge from the vSphere Client. By default, all services are stopped, or in Not Configured state.

**NOTE** You should configure a service before starting it.

**To manage services on a vShield Edge**

1 In the vSphere Client, go to Inventory > Networking.
2 Select an internal port group that is protected by a vShield Edge.
3 Click the vShield Edge tab.
4 Click the Status link.
5 Under Edge Services, select a service and click Start to start the service. Select a service and click Stop to stop a running service.
6 If a service has been started but is not responding, click Refresh Status to send a synchronization request from the vShield Manager. to the vShield Edge.

Upgrade vShield Edge Software

You upgrade the vShield Edge software on a per vShield Edge basis. vShield Edge upgrades must be performed separately from vShield Manager-based upgrades.

**To upgrade vShield Edge software**

1 In the vSphere Client, go to Inventory > Networking.
2 Select an internal port group that is protected by a vShield Edge.
3 Click the vShield Edge tab.
4 Click the Status link.
5 To the right of the Configuration heading, determine if there is a new version to the right of the Upgrade link.
6 Click Upgrade to to locate and install the upgrade file.
vShield Edge and Port Group Isolation
vShield App and vShield Endpoint
vShield App is an interior, vNIC-level firewall that allows you to create access control policies regardless of network topology. A vShield App monitors all traffic in and out of an ESX host, including between virtual machines in the same port group. vShield App includes traffic analysis and container-based policy creation.

vShield App installs as a hypervisor module and firewall service virtual appliance. vShield App integrates with ESX hosts through VMsafe APIs and works with VMware vSphere platform features such as DRS, vMotion, DPM, and maintenance mode.

vShield App provides firewalling between virtual machines by placing a firewall filter on every virtual network adapter. The firewall filter operates transparently and does not require network changes or modification of IP addresses to create security zones. You can write access rules by using vCenter containers, like datacenters, cluster, resource pools and vApps, or network objects, like Port Groups and VLANs, to reduce the number of firewall rules and make the rules easier to track.

You can monitor the health of vShield App instances by using the vShield Manager user interface and by sending vShield App system events to a syslog server.

This chapter includes the following topics:

- “Send vShield App System Events to a Syslog Server” on page 61
- “Back Up the Running CLI Configuration of a vShield App” on page 62
- “View the Current System Status of a vShield App” on page 62

Send vShield App System Events to a Syslog Server

You can send vShield App system events to a syslog server.

To send vShield App system events to a syslog server

1. Log in to the vShield Manager user interface.
2. Select a vShield App from the inventory panel.
3. Click the Configuration tab.
4. Click Syslog Servers.
5. Type the IP address of the syslog server.
6. From the Log Level drop-down menu, select the event level at and above which to send vShield App events to the syslog server.
   
   For example, if you select Emergency, then only emergency-level events are sent to the syslog server. If you select Critical, then critical-, alert-, and emergency-level events are sent to the syslog server.
7. Click Add to save new settings. You send vShield App events to up to five syslog instances.
Back Up the Running CLI Configuration of a vShield App

The CLI Configuration option displays the running configuration of the vShield App. You can back up the running configuration to the vShield Manager to preserve the configuration.

To back up the running CLI configuration of a vShield App

1. Log in to the vShield Manager user interface.
2. Select a vShield App from the inventory panel.
3. Click the Configuration tab.
4. Click CLI Configuration.
5. Click Backup Configuration.

The configuration is populated in the Backup Configuration field. You can cut and paste this text into the vShield App CLI at the Configuration mode prompt.

View the Current System Status of a vShield App

The System Status option lets you view and influence the health of a vShield App. Details include system statistics, status of interfaces, software version, and environmental variables.

To view the health of a vShield App

1. Log in to the vShield Manager user interface.
2. Select a vShield App from the inventory panel.
3. Click the Configuration tab.
4. Click System Status.

From the System Status screen, you can perform the following actions:

- “Force a vShield App to Synchronize with the vShield Manager” on page 62
- “Restart a vShield App” on page 63
- “View Traffic Statistics by vShield App Interface” on page 63

Force a vShield App to Synchronize with the vShield Manager

The Force Sync option forces a vShield App to re-synchronize with the vShield Manager. This might be necessary after a software upgrade.

To force a vShield App to re-synchronize with the vShield Manager

1. Log in to the vShield Manager user interface.
2. Select a vShield App from the inventory panel.
3. Click the Configuration tab.
4. Click System Status.
5. Click Force Sync.
Restart a vShield App

You can restart a vShield App to troubleshoot an operational issue.

**To restart a vShield App**
1. Log in to the vShield Manager user interface.
2. Select a vShield App from the inventory panel.
3. Click the Configuration tab.
4. Click System Status.
5. Click Restart.
6. Click OK in the pop-up window to confirm reboot.

View Traffic Statistics by vShield App Interface

You can view the traffic statistics for each vShield interface.

**To view traffic statistics by vShield port**
1. Log in to the vShield Manager user interface.
2. Select a vShield App from the inventory panel.
3. Click the Configuration tab.
4. Click System Status.
5. Click an interface under the Port column to view traffic statistics.
   
     For example, to view the traffic statistics for the vShield App management interface, click mgmt.
Flow Monitoring is a traffic analysis tool that provides a detailed view of the traffic on your virtual network that passed through a vShield App. The Flow Monitoring output defines which machines are exchanging data and over which application. This data includes the number of sessions, packets, and bytes transmitted per session. Session details include sources, destinations, direction of sessions, applications, and ports being used. Session details can be used to create App Firewall allow or deny rules.

You can use Flow Monitoring as a forensic tool to detect rogue services and examine outbound sessions.

This chapter includes the following topics:

- “Using Flow Monitoring” on page 65
- “View a Specific Application in the Flow Monitoring Charts” on page 66
- “Change the Date Range of the Flow Monitoring Charts” on page 66
- “View the Flow Monitoring Report” on page 66
- “Add an App Firewall Rule from the Flow Monitoring Report” on page 67
- “Editing Port Mappings” on page 68

Using Flow Monitoring

The Flow Monitoring tab displays throughput statistics as returned by a vShield App. Flow Monitoring displays traffic statistics in three charts:

- Sessions/hr: Total number of sessions per hour
- Server KBytes/hr: Number of outgoing kilobytes per hour
- Client/hr: Number of incoming kilobytes per hour

Flow Monitoring organizes statistics by the application protocols used in client-server communications, with each color in a chart representing a different application protocol. This charting method enables you to track your server resources per application.

Traffic statistics display all inspected sessions within the time span specified. The last seven days of data are displayed by default.
View a Specific Application in the Flow Monitoring Charts

You can select a specific application to view in the charts by clicking the Application drop-down menu.

To view the data for a specific application in the Flow Monitoring charts
1 In the vSphere Client, go to Inventory > Hosts and Clusters.
2 Select a datacenter or cluster resource from the resource tree.
3 Click the vShield App tab.
4 Click Flow Monitoring.
5 From the Application drop-down menu, select the application to view.
   The Flow Monitoring charts are refreshed to show data corresponding to the selected application.

Change the Date Range of the Flow Monitoring Charts

You can change the date range of the Flow Monitoring charts for an historical view of traffic data.

To change the date range of the Flow Monitoring chart
1 In the vSphere Client, go to Inventory > Hosts and Clusters.
2 Select a datacenter or cluster resource from the resource tree.
3 Click the vShield App tab.
4 Click Flow Monitoring.
   The charts are updated to display the most current information for the last seven days. This might take several seconds.
5 In the Start Date field, type a new date.
   This date represents the date furthest in the past on which to start the query.
6 Type a new date in the End Date field.
   This represents the most recent date on which to stop the query.
7 Click Update Chart.

View the Flow Monitoring Report

The Flow Monitoring report presents the traffic statistics in tabular format. The report supports drilling down into traffic statistics based on the following hierarchy:

1 Select the firewall action: Allowed or Blocked.
2 Select an L4 or L2/L3 protocol.
   - L4: TCP or UDP
   - L2/L3: ICMP, Other-IPv4, or ARP
3 If an L2/L3 protocol was selected, select an L2/L3 protocol or message type.
4 Select the traffic direction: Incoming, Outgoing, or Intra (between virtual machines).
5 Select the port type: Categorized (standardized ports) or Uncategorized (non-standardized ports).
6 Select an application protocol or port.
7 Select a destination IP address.
8 Select a source IP address.

At the source IP address level, you can create an App Firewall rule based on the specific source and destination IP addresses.

**To view the Flow Monitoring report**

1 In the vSphere Client, go to Inventory > Hosts and Clusters.
2 Select a datacenter or cluster resource from the resource tree.
3 Click the vShield App tab.
4 Click Flow Monitoring.

The charts update to display the most current information for the last seven days. This might take several seconds.
5 Click Show Report.
6 Drill down into the report.
7 Click Show Latest to update the report statistics.

**Add an App Firewall Rule from the Flow Monitoring Report**

By drilling down into the traffic data, you can evaluate the use of your resources and send session information to App Firewall to create a new Layer 4 allow or deny rule. App Firewall rule creation from Flow Monitoring data is available at the datacenter and cluster levels only.

**To add an App Firewall rule from the Flow Monitoring report**

1 In the vSphere Client, go to Inventory > Hosts and Clusters.
2 Select a datacenter resource from the resource tree.
3 Click the vShield App tab.
4 Click Flow Monitoring.

The charts update to display the most current information for the last seven days. This might take several seconds.
5 Click Show Report.
6 Expand the firewall action list.
7 Expand the Layer 4 protocol list.
8 Expand the traffic direction list.
9 Expand the port type list.
10 Expand the application or port list.
11 Expand the destination IP address list.
12 Review the source IP addresses.
13 Select the Zones Firewall column radio button for a source IP address to create an App Firewall rule.

A pop-up window opens. Click Ok to proceed.

The App Firewall table appears. A new table row is displayed at the bottom of the Data Center Low Precedence Rules or Cluster Level Rules section with the session information completed.
14 (Optional) Double-click the Action column cell to change the value to Allow or Deny.

15 (Optional) With the new row selected, click Up to move the rule up in priority.

16 (Optional) Select the Log check box to log all sessions matching this rule.

17 Click Commit to save the rule.

Delete All Recorded Flows

At the datacenter level, you can delete the data for all recorded traffic sessions within the datacenter. This clears the data from charts, the report, and the database. Typically, this is only used when moving your vShield Zones deployment from a lab environment to a production environment. If you must maintain a history of traffic sessions, do not use this feature.

To delete traffic statistics for a datacenter

1 Select a datacenter resource from the inventory panel.
2 Click the Flow Monitoring tab.
3 Click Delete All Flows.
4 Click Ok in the pop-up window to confirm deletion.

CAUTION You cannot recover traffic data after you click Delete All Flows.

Editing Port Mappings

When you click Edit Port Mappings, a table appears, listing well-known applications and protocols, their respective ports, and a description. vShield recognizes common protocol and port mappings, such as HTTP over port 80. Your organization might employ an application or protocol that uses a non-standard port. In this case, you can use Edit Port Mappings to identify a custom protocol-port pair. Your custom mapping appears in the Flow Monitoring report output.

The Edit Port Mappings table offers complete management capabilities, and provides a model for you to follow. You cannot edit or delete the default entries.

Add an Application-Port Pair Mapping

You can add a custom application-port mapping to the port mappings table.

To add an application port-pair mapping

1 Go to Inventory > Networking in the vSphere Client.
2 Select a port group from the inventory panel.
3 Click the Flow Monitoring tab.
4 Click Edit Port Mappings.
5 Click a row in the table.
6 Click Add.

A new row is inserted above the selected row.

7 Double-click the Application cell and type the application name.
8 Double-click the Port Number cell and type the port number.
9 Double-click the Protocol cell to select the transport protocol.
10 Double-click the Resource cell to select the container in which to enforce the new mapping.
   The ANY value adds the port mapping to all containers.
11 Double-click the Description cell and type a brief description.
12 Click Hide Port Mappings.

Delete an Application-Port Pair Mapping
You can delete any application-port pair mapping from the table. When you delete a mapping, any traffic to
the application-port pair is listed as Uncategorized in the Flow Monitoring statistics.

   To delete an application-port pair mapping
   1 Go to Inventory > Networking in the vSphere Client.
   2 Select a port group from the inventory panel.
   3 Click the Flow Monitoring tab.
   4 Click Edit Port Mappings.
   5 Click a row in the table.
   6 Click Delete to delete it from the table.

Hide the Port Mappings Table
When you click Edit Port Mappings, the label changes from Edit Port Mappings to Hide Port Mappings. Click
Hide Port Mappings.
vShield App provides firewall protection through access policy enforcement. The App Firewall tab represents the vShield App firewall access control list.

**NOTE** App Firewall rules apply to vShield App instances, but not vShield Edge or vShield Endpoint instances. The Zones Firewall tab becomes the App Firewall tab when the vShield App license is activated.

This chapter includes the following topics:
- “Using App Firewall” on page 71
- “Create an App Firewall Rule” on page 73
- “Create a Layer 2/Layer 3 App Firewall Rule” on page 75
- “Creating and Protecting Security Groups” on page 75
- “Validating Active Sessions against the Current App Firewall Rules” on page 76
- “Revert to a Previous App Firewall Configuration” on page 77
- “Delete an App Firewall Rule” on page 77
- “Using SpoofGuard” on page 77

**Using App Firewall**

The App Firewall service is a centralized, hierarchical firewall for ESX hosts. App Firewall enables you to create rules that allow or deny access to and from your virtual machines. Each installed vShield App enforces the App Firewall rules.

You can manage App Firewall rules at the datacenter, cluster, and port group levels to provide a consistent set of rules across multiple vShield App instances under these containers. As membership in these containers can change dynamically, App Firewall maintains the state of existing sessions without requiring reconfiguration of firewall rules. In this way, App Firewall effectively has a continuous footprint on each ESX host under the managed containers.

**Securing Containers and Designing Security Groups**

When creating App Firewall rules, you can create rules based on traffic to or from a specific container that encompasses all of the resources within that container. For example, you can create a rule to deny any traffic from inside of a cluster that targets a specific destination outside of the cluster. You can create a rule to deny any incoming traffic that is not tagged with a VLAN ID. When you specify a container as the source or destination, all IP addresses within that container are included in the rule.
A security group is a trust zone that you create and assign resources to for App Firewall protection. Security groups are containers, like a vApp or a cluster. Security groups enables you to create a container by assigning resources arbitrarily, such as virtual machines and network adapters. After the security group is defined, you add the group as a container in the source or destination field of an App Firewall rule. See “Creating and Protecting Security Groups” on page 75.

**Default Rules**

By default, the App Firewall enforces a set of rules allowing traffic to pass through all vShield App instances. These rules appear in the Default Rules section of the App Firewall table. The default rules cannot be deleted or added to. However, you can change the **Action** element of each rule from **Allow** to **Deny**.

**Layer 4 Rules and Layer 2/Layer 3 Rules**

The **App Firewall** tab offers two sets of configurable rules: L4 (Layer 4) rules and L2/L3 (Layer 2/Layer 3) rules. Layers refer to layers of the Open Systems Interconnection (OSI) Reference Model.

Layer 4 rules govern TCP and UDP transport of Layer 7, or application-specific, traffic. Layer 2/Layer 3 rules monitor traffic from ICMP, ARP, and other Layer 2 and Layer 3 protocols. You can configure Layer 2/Layer 3 rules at the datacenter level only. By default, all Layer 4 and Layer 2/Layer 3 traffic is allowed to pass.

**Hierarchy of App Firewall Rules**

Each vShield App enforces App Firewall rules in top-to-bottom ordering. A vShield App checks each traffic session against the top rule in the App Firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced.

The rules are enforced in the following hierarchy:

1. **Data Center High Precedence Rules**
2. **Cluster Level Rules**
3. **Data Center Low Precedence Rules** (seen as Rules below this level have lower precedence than cluster level rules when a datacenter resource is selected)
4. **Secure Port Group Rules**
5. **Default Rules**

App Firewall offers container-level and custom priority precedence configurations:

- **Container-level precedence** refers to recognizing the datacenter level as being higher in priority than the cluster level. When a rule is configured at the datacenter level, the rule is inherited by all clusters and vShield agents therein. A cluster-level rule is only applied to the vShield App within the cluster.

- **Custom priority precedence** refers to the option of assigning high or low precedence to rules at the datacenter level. High precedence rules work as noted in the container-level precedence description. Low precedence rules include the Default Rules and the configuration of Data Center Low Precedence rules. This flexibility allows you to recognize multiple layers of applied precedence.

At the cluster level, you configure rules that apply to all vShield App instances within the cluster. Because Data Center High Precedence Rules are above Cluster Level Rules, ensure your Cluster Level Rules are not in conflict with Data Center High Precedence Rules.

**Planning App Firewall Rule Enforcement**

Using App Firewall, you can configure allow and deny rules based on your network policy. The following examples represent two common firewall policies:

- **Allow all traffic by default.** You keep the default allow all rules and add deny rules based on Flow Monitoring data or manual App Firewall rule configuration. In this scenario, if a session does not match any of the deny rules, the vShield App allows the traffic to pass.
Deny all traffic by default. You can change the Action status of the default rules from Allow to Deny, and add allow rules explicitly for specific systems and applications. In this scenario, if a session does not match any of the allow rules, the vShield App drops the session before it reaches its destination. If you change all of the default rules to deny any traffic, the vShield App drops all incoming and outgoing traffic.

Create an App Firewall Rule

App Firewall rules allow or deny traffic based on the following criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source (A.B.C.D/nn)</td>
<td>Container, direction in relation to container, or IP address with netmask (nn) from which the communication originated.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Port or range of ports from which the communication originated. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.</td>
</tr>
<tr>
<td>Destination (A.B.C.D/nn)</td>
<td>Container, direction in relation to container, or IP address with netmask (nn) which the communication is targeting.</td>
</tr>
<tr>
<td>Destination Application</td>
<td>The application on the destination the source is targeting. If you select a protocol from the drop-down list, the well-known port for the selected protocol appears in the Destination Port field.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port or range of ports which the communication is targeting. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol used for communication.</td>
</tr>
</tbody>
</table>

You can add destination and source port ranges to a rule for dynamic services such as FTP and RPC, which require multiple ports to complete a transmission.

To create a firewall rule at the datacenter level

1. In the vSphere Client, go to Inventory > Hosts and Clusters.
2. Select a datacenter resource from the resource tree.
3. Click the vShield App tab.
4. Click App Firewall.
   By default, the L4 Rules option is selected.
   To create L2/L3 rules, see “Create a Layer 2/Layer 3 App Firewall Rule” on page 75.
5. Do one of the following:
   - Click Add to add a new rule to the Data Center Low Precedence Rules (Rules below this level have lower precedence...).
   - Select a row in the Data Center High Precedence Rules section of the table and click Add. A new row appears below the selected row.
6. Double-click each cell in the new row to select the appropriate information.
   You can type IP addresses in the Source and Destination fields, and port numbers in the Source Port and Destination Port fields.
7. (Optional) Select the new row and click Up to move the rule up in priority.
8. (Optional) Select the Log check box to log all sessions matching this rule.
9. Click Commit to save the rule.

NOTE Layer 4 firewall rules can also be created from the Flow Monitoring report. See “Add an App Firewall Rule from the Flow Monitoring Report” on page 67.
To create a firewall rule at the cluster level

1. In the vSphere Client, go to Inventory > Hosts and Clusters.
2. Select a cluster resource from the resource tree.
3. Click the vShield App tab.
4. Click App Firewall.
   By default, the L4 Rules option is selected.
   To create L2/L3 rules, see “Create a Layer 2/Layer 3 App Firewall Rule” on page 75.
5. Click Add.
   A new row appears in the Cluster Level Rules section of the table.
6. Double-click each cell in the new row to select the appropriate information.
   You can type IP addresses in the Source and Destination fields, and port numbers in the Source Port and Destination Port fields.
7. (Optional) Select the new row and click Up to move the row up in priority.
8. (Optional) Select the Log check box to log all sessions matching this rule.
9. Click Commit to save the rule.

NOTE Layer 4 firewall rules can also be created from the Flow Monitoring report. See “Add an App Firewall Rule from the Flow Monitoring Report” on page 67.

To create a firewall rule at the port group level

1. In the vSphere Client, go to Inventory > Networking.
2. Select a port group from the resource tree.
3. Click the vShield App tab.
4. Click App Firewall.
5. Click Add.
   A new row is added at the bottom of the Secure Port Group Rules section.
6. Double-click each cell in the new row to select the appropriate information.
   You can type IP addresses in the Source and Destination fields, and port numbers in the Source Port and Destination Port fields.
7. (Optional) Select the new row and click Up to move the row up in priority.
8. (Optional) Select the Log check box to log all sessions matching this rule.
9. Click Commit to save the rule.

NOTE Layer 4 firewall rules can also be created from the Flow Monitoring report. See “Add an App Firewall Rule from the Flow Monitoring Report” on page 67.
Create a Layer 2/Layer 3 App Firewall Rule

The Layer 2/Layer 3 firewall enables configuration of allow or deny rules for common Data Link Layer and Network Layer requests, such as ICMP pings and traceroutes. You can change the default Layer 2/Layer 3 rules from allow to deny based on your network security policy.

Layer 2/Layer 3 firewall rules allow or deny traffic based on the following criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source (A.B.C.D/nn)</td>
<td>Container, direction in relation to container, or IP address with netmask (nn) from which the communication originated</td>
</tr>
<tr>
<td>Destination (A.B.C.D/nn)</td>
<td>Container, direction in relation to container, or IP address with netmask (nn) which the communication is targeting</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol used for communication</td>
</tr>
</tbody>
</table>

To create a Layer 2/Layer 3 firewall rule

1. In the vSphere Client, go to Inventory > Hosts and Clusters.
2. Select a datacenter resource from the resource tree.
3. Click the vShield App tab.
4. Click App Firewall.
5. Click L2/L3 Rules.
6. Click Add.
   A new row is added at the bottom of the DataCenter Rules section of the table.
7. Double-click each cell in the new row to type or select the appropriate information.
   You can type IP addresses in the Source and Destination fields.
8. (Optional) Select the Log check box to log all sessions matching this rule.
9. Click Commit.

**NOTE** Layer 2/Layer 3 firewall rules can also be created from the Flow Monitoring report. See “Add an App Firewall Rule from the Flow Monitoring Report” on page 67.

Creating and Protecting Security Groups

The Security Groups feature enables you to create custom containers to which you can assign resources, such as virtual machines and network adapters, for App Firewall protection. After a security group is defined, you add the security group to a firewall rule for protection.

Add a Security Group

In the vSphere Client, you can add a security group at the datacenter resource level.

To add a security group by using the vSphere Client

1. Click a datacenter resource from the vSphere Client.
2. Click the vShield App tab.
3. Click Security Groups.
4. Click Add Group.
5 Double-click the row and type a name for the group.
6 Click Add.

After security group creation is complete, assign resources to the group.

**Assign Resources to a Security Group**

You can assign virtual machines and network adapters to a security group. These resources have associated IP addresses that define the source or destination parameters for which an App Firewall rule enforces an access policy.

**To assign resources to a security group**

1 Click a datacenter resource from the vSphere Client.
2 Click the vShield App tab.
3 Click Security Groups.
4 Click the arrow next to the name of a security group to expand the details of the group.
5 Select a vNIC from the drop-down list and click Add.
   The selected vNIC appears under vNIC Membership.
   Repeat these steps for each vNIC you want to place in this security group.
6 Click Commit.

After assigning resources, add the security group to a firewall rule as a container. See “Create an App Firewall Rule” on page 73.

**Validating Active Sessions against the Current App Firewall Rules**

By default, a vShield Edge matches firewall rules against each new session. After a session has been established, any firewall rule changes do not affect active sessions.

The CLI command `validate sessions` enables you to validate active sessions that are in violation of the current rule set. You would use this procedure for the following scenarios:

- You updated the firewall rule set. After a firewall rule set update, you should validate active sessions to purge any existing sessions that are in violation of the updated policy.
- You viewed sessions in Flow Monitoring and determined that an existing or historical flow requires a new access rule. After creating a firewall rule that matches the offending session, you should validate active sessions to purge any existing sessions that are in violation of the updated policy.

After the App Firewall update is complete, issue the `validate sessions` command from the CLI of a vShield App to purge sessions that are in violation of current policy.

**To validate active sessions against the current firewall rules**

1 Update and commit the App Firewall rule set at the appropriate container level.
2 Open a console session on a vShield App issue the `validate sessions` command.

```
vShieldApp> enable
Password: 
vShieldApp# validate sessions
```
Revert to a Previous App Firewall Configuration

The vShield Manager saves a snapshot of App Firewall settings each time you commit a new rule. Clicking **Commit** causes the vShield Manager to save the previous configuration with a timestamp before adding the new rule. These snapshots are available from the **Revert to Snapshot** drop-down list.

**To revert to a previous App Firewall configuration**

1. In the vSphere Client, go to **Inventory > Hosts and Clusters**.
2. Select a datacenter or cluster resource from the inventory panel.
3. Click the **vShield App** tab.
4. Click **App Firewall**.
5. From the **Revert to Snapshot** drop-down list, select a snapshot.
   - Snapshots are presented in the order of timestamps, with the most recent snapshot listed at the top.
6. View snapshot configuration details.
7. Do one of the following:
   - To return to the current configuration, select the - option from the **Revert to Snapshot** drop-down list.
   - Click **Commit** to overwrite the current configuration with the snapshot configuration.

Delete an App Firewall Rule

You can delete any App Firewall rule you have created. You cannot delete the any rules in the Default Rules section of the table.

**To delete an App Firewall rule**

1. Click an existing row in the App Firewall table.
2. Click **Delete**.
3. Click **Commit**.

Using SpoofGuard

After synchronizing with the vCenter Server, the vShield Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine. Up to vShield 4.1, vShield trusted the IP address provided by VMware Tools on a virtual machine. However, if a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

SpoofGuard allows you to authorize the IP addresses reported by VMware Tools, and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vsphere SDK. Operating separately from the App Firewall rules, you can use SpoofGuard to block traffic determined to be spoofed.

When enabled, you can use SpoofGuard to monitor and manage the IP addresses reported by your virtual machines in one of the following modes.

- **Automatically Trust IP Assignments On Their First Use**: This mode allows all traffic from your virtual machines to pass while building a table of MAC-to-IP address assignments. You can review this table at your convenience and make IP address changes.

- **Manually Inspect and Approve All IP Assignments Before Use**: This mode blocks all traffic until you approve each MAC-to-IP address assignment.

**NOTE** SpoofGuard inherently allows DHCP requests regardless of enabled mode. However, if in manual inspection mode, traffic does not pass until the DHCP-assigned IP address has been approved.
SpoofGuard Screen Options

The SpoofGuard screen displays the following options.

### Table 13-1. SpoofGuard Screen Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Status</td>
<td>Status of SpoofGuard as either enabled or disabled</td>
</tr>
<tr>
<td>Inactive</td>
<td>List of IP addresses where the current IP address does not match the published IP address.</td>
</tr>
<tr>
<td>Active Since Last Published</td>
<td>List of IP addresses that have been validated since the policy was last updated</td>
</tr>
<tr>
<td>Unpublished IP assignment changes</td>
<td>List of virtual machines for which you have edited the IP address assignment but have not yet published</td>
</tr>
<tr>
<td>Require Approval</td>
<td>IP address changes that require approval before traffic can flow to or from these virtual machines</td>
</tr>
<tr>
<td>Duplicate IP assignments</td>
<td>IP addresses that are duplicates of an existing assigned IP address within the selected datacenter</td>
</tr>
</tbody>
</table>

Enable SpoofGuard

You must enable SpoofGuard per datacenter to manage IP address assignments.

**IMPORTANT** You must upgrade all vShield App instances to vShield App 1.0.0 Update 1 or later before you enable SpoofGuard.

**To enable SpoofGuard**

1. In the vShield Manager user interface, go to the **Hosts and Clusters** view.
2. Select a datacenter resource from the resource tree.
3. Click the **SpoofGuard** tab.
4. Click **Edit** to the right side of the Global Status heading.
5. For **IP Assignment Tracking**, click **Enabled**.
6. For **Operation Mode**, select one of the following:
   - **Automatically Trust IP Assignments on Their First Use**: Select this option to trust all IP assignments upon initial registration with the vShield Manager.
   - **Manually Inspect and Approve All IP Assignments Before Use**: Select this option to require manual approval of all IP addresses. All traffic to and from unapproved IP addresses is blocked.
7. Click **Ok**.

Approve IP Addresses

If you set SpoofGuard to require manual approval of all IP address assignments, you must approve IP address assignments to allow traffic from those virtual machines to pass.

**To approve an IP address**

1. In the vShield Manager user interface, go to the **Hosts and Clusters** view.
2. Select a datacenter resource from the resource tree.
3. Click the **SpoofGuard** tab.
4. Click the **Require Approval** or **Duplicate IP assignments** link.
5 Do one of the following:
   - Select the top check box in the left side check box column to select all assignments on the screen.
   - Select the check box for each assignment you are ready to approve.

6 Click Approve Selected.
7 Click Publish Changes.

## Edit an IP Address

You can edit the IP address assigned to a MAC address to correct the assigned IP address.

**NOTE** SpoofGuard accepts a unique IP address from more than virtual machine. However, you can assign an IP address only once. An approved IP address is unique across the vShield system. Duplicate approved IP addresses are not allowed.

### To edit an IP address

1 In the vShield Manager user interface, go to the **Hosts and Clusters** view.
2 Select a datacenter resource from the resource tree.
3 Click the **SpoofGuard** tab.
4 Click one of the option links.
5 In the Approved IP column, click **Edit**.
6 Type an IP address in the **Approved IP Address** pop-up window.
7 Click **Apply**.
8 Click **Publish Changes**.

## Delete an IP Address

You can delete a MAC-to-IP address assignment from the SpoofGuard table to clean the table of a virtual machine that is no longer active. Any deleted instance can reappear in the SpoofGuard table based on viewed traffic and the current enabled state of SpoofGuard.

### To delete an IP address

1 In the vShield Manager user interface, go to the **Hosts and Clusters** view.
2 Select a datacenter resource from the resource tree.
3 Click the **SpoofGuard** tab.
4 Click one of the option links.
5 In the Approved IP column, click **Delete**.
6 Click **Publish Changes**.
vShield Endpoint delivers an introspection-based antivirus solution. vShield Endpoint uses the hypervisor to scan guest virtual machines from the outside without a bulky agent. vShield Endpoint is efficient in avoiding resource bottlenecks while optimizing memory use.

vShield Endpoint health status is conveyed by using alarms that show in red and yellow on the vCenter Server console. In addition, more status information can be gathered by looking at the event logs.

**IMPORTANT** Your vCenter Server must be correctly configured for vShield Endpoint security:

- Not all guest operating systems are supported by vShield Endpoint. Virtual machines with non-supported operating systems are not protected by the security solution.
- All virtual machines (with supported operating systems) that reside on a vShield Endpoint-protected ESX host must be protected by a vShield Endpoint module.
- Not all ESX hosts in a vCenter Server must be protected by the security solution, but each protected ESX must have an SVM installed on it.

**CAUTION** vMotion migration of a protected virtual machine are blocked if the target ESX is not enabled for vShield Endpoint. Make sure that the resource pool for vMotion of protected virtual machines contains only security enabled ESX hosts.

This chapter includes the following topics:

- “View vShield Endpoint Status” on page 81
- “Alarms” on page 82
- “Events” on page 83
- “Audit Messages” on page 86

**View vShield Endpoint Status**

Monitoring a vShield Endpoint instance involves checking for status coming from the vShield Endpoint components: the security virtual machine (SVM), the ESX host-resident vShield Endpoint module, and the protected virtual machine-resident thin agent.

**To view vShield Endpoint status**

1. In the vSphere Client, go to Inventory > Hosts and Clusters.
2. Select a datacenter, cluster, or ESX host resource from the resource tree.
3. Click the vShield App tab (or vShield tab on ESX hosts).
4. Click Endpoint Status.
Alarms

Alarms signal the vCenter Server administrator about vShield Endpoint events that require attention. Alarms are automatically cancelled in case the alarm state is no longer present.

vCenter Server alarms can be displayed without a custom vSphere plug-in. See the vCenter Server Administration Guide on events and alarms.

Upon registering as a vCenter Server extension, the vShield Manager defines the rules that create and remove alarms, based on events coming from the three vShield Endpoint components: SVM, vShield Endpoint module, and thin agent. Rules can be customized. For instructions on how to customize rules for alarms, see the vCenter Server documentation. In some cases, there are multiple possible causes for the alarm. The tables that follow list the possible causes and the corresponding actions you might want to take for remediation.

vShield Endpoint defines three sets of alarms:

- "Host Alarms" on page 82
- "SVM Alarms" on page 82
- "VM Alarms" on page 83

Host Alarms

Host alarms are generated by events affecting the health status of the vShield Endpoint module.

**Table 14-1. Warnings (Marked Yellow)**

<table>
<thead>
<tr>
<th>Possible Cause</th>
<th>Action</th>
</tr>
</thead>
</table>
| SVM is registered, but vShield Endpoint module does not see any virtual machines to protect. No requests for protection are coming from any virtual machines. No virtual machines are currently protected. | - Usually a transient state occurring while existing virtual machines are being moved with vMotion, or are just coming up. No action required.  
- The ESX host has no virtual machines yet, or only virtual machines with non-supported operating systems. No action required.  
- Check the vShield Manager console for the status of the virtual machines that should be protected on that host. If one or more have an error status, the Endpoint thin agents in those machines may be malfunctioning. |

**Table 14-2. Errors (Marked Red)**

<table>
<thead>
<tr>
<th>Possible Cause</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SVM version is not compatible with the vShield Endpoint module version.</td>
<td>Install compatible components. Look in the vShield Endpoint Installation Guide for compatible versions for vShield Endpoint module and SVM.</td>
</tr>
</tbody>
</table>

SVM Alarms

SVM alarms are generated by events affecting the health status of the vShield Endpoint module.

**Table 14-3. Red SVM Alarms**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The vShield Monitor is not receiving status from the SVM.</td>
<td>Either there are network issues between the vShield Monitor and the SVM, or the SVM is not operating properly.</td>
</tr>
<tr>
<td>The SVM failed to initialize</td>
<td>Contact your security provider for help with SVM errors.</td>
</tr>
</tbody>
</table>
VM Alarms

VM alarms are generated by events affecting the health status of the vShield Endpoint module.

Table 14-4. Warnings

<table>
<thead>
<tr>
<th>Possible Cause</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SVM is overloaded. The virtual machines will not be protected while the alarm persists.</td>
<td>Check resources allocation for the SVM and allocate more resources, if necessary. Check the vCenter Server event log for the ESX the SVM is attached to. An event code of 1002 can indicate an overloaded SVM.</td>
</tr>
<tr>
<td>The thin agent in one or more virtual machines is initialized but not reporting events. Those virtual machines are not protected while this warning persists.</td>
<td>This is usually a transient alarm that does not require attention. If it persists or turns to red, look at the vCenter Server event log for the protected VM. An event code of 1000 indicates a non-functioning thin agent.</td>
</tr>
</tbody>
</table>

Table 14-5. Errors

<table>
<thead>
<tr>
<th>Possible Cause</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The thin agent version is not compatible with the vShield Endpoint module</td>
<td>Install compatible components. Look in the vShield Endpoint Installation Guide for compatible versions for vShield Endpoint module and SVM.</td>
</tr>
<tr>
<td>The thin agent is not reporting vShield Endpoint events. The virtual machine is not protected.</td>
<td>The thin agent is malfunctioning, or not initialized. Look at the event log to see if the thin agent was initialized successfully.</td>
</tr>
<tr>
<td>The virtual machine is still powered on, but the thin agent is disabled. The virtual machine is not protected.</td>
<td>If the error persists, this thin agent is malfunctioning. (A virtual machine that is shutting down or in the process of a vMotion move does not generate a red alarm.)</td>
</tr>
</tbody>
</table>

Events

Events are used for logging and auditing conditions inside the vShield Endpoint-based security system.

Events can be displayed without a custom vSphere plug-in. See the vCenter Server Administration Guide on events and alarms.

Events are the basis for alarms that are generated. Upon registering as a vCenter Server extension, the vShield Manager defines the rules that create and remove alarms.

Default base arguments for an event are the reported time and the vShield Manager event_id.

Table 14-6 lists vShield Endpoint events reported by the SVM and the vShield Manager (VSM) in order by code number. The table shows the even code, name, the VC arguments, the event category, and a description. In the Event Category column, events that generate error alarms are colored red. Events that generate warning alarms are colored yellow.

Table 14-6. vShield Endpoint Events

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>VC Arguments</th>
<th>Event Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>VSM_FSFD_EVENT_VERSION_MISMATCH</td>
<td>timestamp, SVM version of FSFD protocol, FSFD version of FSFD protocol</td>
<td>error</td>
<td>vShield Endpoint: The SVM was contacted by a non-compatible version of the vShield Endpoint Thin Agent.</td>
</tr>
<tr>
<td>0003</td>
<td>VSM_FSFD_EVENT_DISK_FULL</td>
<td>timestamp</td>
<td>warning</td>
<td>The vShield Endpoint Thin Agent encountered a “disk full” error while attempting to write to the local disk.</td>
</tr>
<tr>
<td>0004</td>
<td>VSM_FSFD_EVENT_TIMEOUT</td>
<td>timestamp</td>
<td>warning</td>
<td>A timeout occurred in the communication between the SVM and the Thin Agent.</td>
</tr>
</tbody>
</table>
Table 14-6. vShield Endpoint Events (Continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>VC Arguments</th>
<th>Event Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0005</td>
<td>VSM_FSFD_EVENT_UNKNOWN_STATE</td>
<td>timestamp</td>
<td>warning</td>
<td>N/A</td>
</tr>
<tr>
<td>0006</td>
<td>VSM_FSFD_EVENT_MISSING_TIMER</td>
<td>timestamp</td>
<td>error</td>
<td>Lost communication with Thin Agent.</td>
</tr>
<tr>
<td>0007</td>
<td>VSM_FSFD_EVENT_TIMER_RESTORED</td>
<td>timestamp, FSFD version of FSFD protocol</td>
<td>info</td>
<td>Established communication with Thin Agent.</td>
</tr>
<tr>
<td>1000</td>
<td>VSM_VM_EVENT_CONNECTED</td>
<td>timestamp</td>
<td>info</td>
<td>VM has connected with the SVM.</td>
</tr>
<tr>
<td>1001</td>
<td>VSM_VM_EVENT_DISCONNECTED</td>
<td>timestamp</td>
<td>info</td>
<td>VM has disconnected from the SVM.</td>
</tr>
<tr>
<td>1002</td>
<td>VSM_VM_EVENT_UNKNOWN_STATE</td>
<td>timestamp</td>
<td>warning</td>
<td>Thin Agent Health Status Information has been lost.</td>
</tr>
<tr>
<td>N/A</td>
<td>VM_POWERED_OFF</td>
<td>timestamp</td>
<td>info</td>
<td>Detected VM power off.</td>
</tr>
<tr>
<td>2000</td>
<td>VSM_SVM_EVENT_ENABLED</td>
<td>timestamp, SVM version of LKM protocol, SVM version of FSFD protocol, port SVM is listening on</td>
<td>info</td>
<td>SVM enabled.</td>
</tr>
<tr>
<td>2001</td>
<td>VSM_SVM_EVENT_INIT_FAILURE</td>
<td>timestamp</td>
<td>error</td>
<td>SVM initialization failed.</td>
</tr>
<tr>
<td>2003</td>
<td>VSM_SVM_EVENT_FSFD_FLOOD_DETECTED</td>
<td>timestamp</td>
<td>warning</td>
<td>SVM detected high volume of vShield Endpoint events.</td>
</tr>
<tr>
<td>2005</td>
<td>VSM_SVM_EVENT_DROPPED_EVENTS</td>
<td>timestamp</td>
<td>warning</td>
<td>Health Status information has been lost.</td>
</tr>
<tr>
<td>2006</td>
<td>VSM_SVM_EVENT_MISSING_REPORT</td>
<td>timestamp</td>
<td>error</td>
<td>vShield Manager lost communication with SVM.</td>
</tr>
<tr>
<td>2007</td>
<td>VSM_SVM_EVENT_REPORT_RESTORED</td>
<td>timestamp</td>
<td>info</td>
<td>vShield Manager communication with SVM have been restored.</td>
</tr>
<tr>
<td>3000</td>
<td>VSM_HOST_EVENT_VERSION_MISMATCH</td>
<td>timestamp, Host version of LKM protocol, Host version of LKM protocol</td>
<td>error</td>
<td>vShield Endpoint: The SVM was contacted by a non-compatible version of the vShield Endpoint module.</td>
</tr>
<tr>
<td>3002</td>
<td>VSM_HOST_EVENT_UNKNOWN_STATE</td>
<td>timestamp</td>
<td>warning</td>
<td>vShield Endpoint Module Status Information has been lost.</td>
</tr>
<tr>
<td>3003</td>
<td>VSM_HOST_EVENT_SVM_REGISTERED</td>
<td>timestamp</td>
<td>info</td>
<td>SVM is registered with the vShield Manager.</td>
</tr>
<tr>
<td>3004</td>
<td>VSM_HOST_EVENT_SVM_UNREGISTERED</td>
<td>timestamp</td>
<td>info</td>
<td>SVM is unregistered with the vShield Manager.</td>
</tr>
<tr>
<td>3005</td>
<td>VSM_HOST_EVENT_VMS_CONNECTED</td>
<td>timestamp, Host version of vShield Endpoint module protocol</td>
<td>info</td>
<td>vShield Endpoint module has connected with SVM.</td>
</tr>
<tr>
<td>3006</td>
<td>VSM_HOST_EVENT_VMS_DISCONNECTED</td>
<td>timestamp</td>
<td>info</td>
<td>vShield Endpoint module has disconnected from the SVM.</td>
</tr>
</tbody>
</table>
Possible causes for events are listed in Table 14-7:

Table 14-7. Possible Causes for Events

<table>
<thead>
<tr>
<th>Code</th>
<th>Event</th>
<th>Possible Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>VSM_FSFD_EVENT_VERSION_MISMATCH</td>
<td>Compatible versions of the vShield Endpoint modules must be used. Please refer to the vShield Endpoint Installation guide for a compatibility list.</td>
</tr>
<tr>
<td>0003</td>
<td>VSM_FSFD_EVENT_DISK_FULL</td>
<td>The vShield Endpoint Thin Agent may need to write to a file on the local disk for file remediation purposes, as well as for temporary storage. The file location for the temporary files is: %SYSTEMROOT%\temp\vmware\eps010\ For remediation purposes, the needed storage is comparable to the size of the file being remediated. It is recommended that local disks are at 95% or less capacity. Running out of disk space may prevent vShield Endpoint from functioning properly and from effectively protecting the affected VM.</td>
</tr>
<tr>
<td>0004</td>
<td>VSM_FSFD_EVENT_TIMEOUT</td>
<td>VM is slow to respond to SVM requests. This may happen when the VM is temporarily running low on CPU resources.</td>
</tr>
<tr>
<td>0005</td>
<td>VSM_FSFD_EVENT_UNKNOWN_STATE</td>
<td>N/A</td>
</tr>
<tr>
<td>0006</td>
<td>VSM_FSFD_EVENT_MISSING_TIMER</td>
<td>Thin agent is not operating properly.</td>
</tr>
<tr>
<td>0007</td>
<td>VSM_FSFD_EVENT_TIMER_RESTORED</td>
<td>N/A</td>
</tr>
<tr>
<td>1000</td>
<td>VSM_VM_EVENT_CONNECTED</td>
<td>VM configured for vShield Endpoint protection will generate this event when loaded on the corresponding ESX host, for example, during power-up or incoming vMotion.</td>
</tr>
<tr>
<td>1001</td>
<td>VSM_VM_EVENT_DISCONNECTED</td>
<td>VM configured for vShield Endpoint protection will generate this event when loaded on the corresponding ESX host, for example, during shutdown or outgoing vMotion.</td>
</tr>
<tr>
<td>1002</td>
<td>VSM_VM_EVENT_UNKNOWN_STATE</td>
<td>Heavy load of event reporting on the SVM, or a communication problem between the SVM and the vShield Manager.</td>
</tr>
<tr>
<td>N/A</td>
<td>VMPOWERED_OFF</td>
<td>N/A</td>
</tr>
<tr>
<td>2000</td>
<td>VSM_VM_EVENT_ENABLED</td>
<td>N/A</td>
</tr>
<tr>
<td>2001</td>
<td>VSM_VM_EVENT_INIT_FAILURE</td>
<td>vShield Endpoint SVM component failed to initialize. Please consult partner SVM installation documentation for causes.</td>
</tr>
<tr>
<td>2003</td>
<td>VSM_VM_EVENT_FSFD_FLOOD_DETECTED</td>
<td>The SVM is overloaded. The number of events exceeds the maximum concurrent events threshold.</td>
</tr>
<tr>
<td>2005</td>
<td>VSM_VM_EVENT_DROPPED_EVENTS</td>
<td>Heavy load of event reporting on the SVM, or communication problem between the SVM and the vShield Manager.</td>
</tr>
<tr>
<td>2006</td>
<td>VSM_VM_EVENT_MISSING_REPORT</td>
<td>1 Check SVM status. 2 Check network connection between vShield Manager and SVM.</td>
</tr>
<tr>
<td>2007</td>
<td>VSM_VM_EVENT_REPORT_RESTOREED</td>
<td>N/A</td>
</tr>
<tr>
<td>3000</td>
<td>VSM_HOST_EVENT_VERSION_MISMATCH</td>
<td>Compatible versions of the vShield Endpoint modules must be used. Please refer to the vShield Endpoint Installation guide for a compatibility list.</td>
</tr>
<tr>
<td>3002</td>
<td>VSM_HOST_EVENT_UNKNOWN_STATE</td>
<td>Heavy load of event reporting on the SVM, or communication problem between the SVM and the vShield Manager.</td>
</tr>
<tr>
<td>3003</td>
<td>VSM_HOST_EVENT_SVM_REGISTERED</td>
<td>N/A</td>
</tr>
<tr>
<td>3004</td>
<td>VSM_HOST_EVENT_SVM_UNREGISTERED</td>
<td>N/A</td>
</tr>
<tr>
<td>3005</td>
<td>VSM_HOST_EVENT_VMS_CONNECTED</td>
<td>N/A</td>
</tr>
<tr>
<td>3006</td>
<td>VSM_HOST_EVENT_VMS_DISCONNECTED</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Audit Messages

Audit messages include fatal errors and other important audit messages and are logged to `vmware.log`. The following conditions are logged as AUDIT messages:

- Thin agent initialization success (and version number.)
- Thin agent initialization failure.
- Successfully found SCSI device to communicate with the security virtual machine (SVM).
- Failure to create filter device object, or failure to attach to device stack.
- Established first time communication with SVM.
- Failure to establish communication with SVM (when first such failure occurs).

Generated log messages have the following substrings near the beginning of each log message: `vf-AUDIT`, `vf-ERROR`, `vf-WARN`, `vf-INFO`, `vf-DEBUG`. 
Appendixes
Each vShield virtual machine contains a command line interface (CLI). This appendix details CLI usage and commands.

User account management in the CLI is separate from user account management in the vShield Manager user interface.

This appendix includes the following topics:

- “Logging In and Out of the CLI” on page 89
- “CLI Command Modes” on page 89
- “CLI Syntax” on page 90
- “Moving Around in the CLI” on page 90
- “Getting Help within the CLI” on page 91
- “Securing CLI User Accounts and the Privileged Mode Password” on page 91
- “Command Reference” on page 93

Logging In and Out of the CLI

Before you can run CLI commands, you must initiate a console session to a vShield virtual machine. To open a console session within the vSphere Client, select the vShield virtual machine from the inventory panel and click the Console tab. You can log in to the CLI by using the default user name admin and password default.

You can also use SSH to access the CLI. By default, SSH access is disabled. Use the ssh command to enable and disable the SSH service on a vShield virtual appliance. See “ssh” on page 102.

To log out, type exit from either Basic or Privileged mode.

CLI Command Modes

The commands available to you at any given time depend on the mode you are currently in.

**NOTE** vShield Edge virtual machines have Basic mode only.

- Basic: Basic mode is a read-only mode. To have access to all commands, you must enter Privileged mode.
- Privileged: Privileged mode commands allow support-level options such as debugging and system diagnostics. Privileged mode configurations are not saved upon reboot. You must run the write memory command to save Privileged mode configurations.
- Configuration: Configuration mode commands allow you to change the current configuration of utilities on a vShield virtual machine. You can access Configuration mode from Privileged mode. From Configuration mode, you can enter Interface configuration mode.

- Interface Configuration: Interface Configuration mode commands allow you to change the configuration of virtual machine interfaces. For example, you can change the IP address and IP route for the management port of the vShield Manager.

### CLI Syntax

Run commands at the prompt as shown. Do not type the ( ), < >, or [ ] symbols.

```
command A.B.C.D (option1 | option2) <0-512> [WORD]
```

- Required numerical ranges are enclosed in angle brackets.
- Required text is presented in all capital letters.
- Multiple, required keywords or options are enclosed in parentheses and separated by a pipe character.
- An optional keyword or value is enclosed in square brackets.

### Moving Around in the CLI

The following commands move the pointer around on the command line.

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL+A</td>
<td>Moves the pointer to beginning of the line.</td>
</tr>
<tr>
<td>CTRL+B or the left arrow key</td>
<td>Moves the pointer back one character.</td>
</tr>
<tr>
<td>CTRL+C</td>
<td>Ends any operation that continues to propagate, such as a ping.</td>
</tr>
<tr>
<td>CTRL+D</td>
<td>Deletes the character at the pointer.</td>
</tr>
<tr>
<td>CTRL+E</td>
<td>Moves the pointer to end of the line.</td>
</tr>
<tr>
<td>CTRL+F or the right arrow key</td>
<td>Moves the pointer forward one character.</td>
</tr>
<tr>
<td>CTRL+K</td>
<td>Deletes all characters from the pointer to the end of the line.</td>
</tr>
<tr>
<td>CTRL+N or the down arrow key</td>
<td>Displays more recent commands in the history buffer after recalling commands with CTRL+P (or the up arrow key). Repeat to recall other recently run commands.</td>
</tr>
<tr>
<td>CTRL+P or the up arrow key</td>
<td>Recalls commands in the history, starting with the most recent completed command. Repeat to recall successively older commands.</td>
</tr>
<tr>
<td>CTRL+U</td>
<td>Deletes all characters from the pointer to beginning of the line.</td>
</tr>
<tr>
<td>CTRL+W</td>
<td>Deletes the word to the left of pointer.</td>
</tr>
<tr>
<td>ENTER</td>
<td>Scrolls down one line.</td>
</tr>
<tr>
<td>ESC+B</td>
<td>Moves the pointer back one word.</td>
</tr>
<tr>
<td>ESC+D</td>
<td>Deletes all characters from the pointer to the end of the word.</td>
</tr>
<tr>
<td>ESC+F</td>
<td>Moves the pointer forward one word.</td>
</tr>
<tr>
<td>SPACE</td>
<td>Scrolls down one screen.</td>
</tr>
</tbody>
</table>
Getting Help within the CLI

The CLI contains the following commands for assisting your use.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Moves the pointer to the beginning of the line.</td>
</tr>
<tr>
<td>sho?</td>
<td>Displays a list of commands that begin with a particular character string.</td>
</tr>
<tr>
<td>exp+TAB</td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td>show ?</td>
<td>Lists the associated keywords of a command.</td>
</tr>
<tr>
<td>show log ?</td>
<td>Lists the associated arguments of a command.</td>
</tr>
<tr>
<td>list</td>
<td>Displays the verbose options of all commands for the current mode.</td>
</tr>
</tbody>
</table>

Securing CLI User Accounts and the Privileged Mode Password

You must manage CLI user accounts separately on each vShield virtual machine. By default, you use the admin user account to log in to the CLI of each vShield virtual machine. The CLI admin account and password are separate from the vShield Manager user interface admin account and password.

You should create a new CLI user account and remove the admin account to secure access to the CLI on each vShield virtual machine.

User account management in the CLI conforms to the following rules.

- You can create CLI user accounts. Each created user account has administrator-level access to the CLI.
- You cannot change the password for any CLI user account on a vShield Manager or vShield App virtual machine. If you need to change a CLI user account password, you must delete the user account, and then re-add it with a new password. You can change the password of any non-admin account on the vShield Edge.

The CLI admin account password and the Privileged mode password are managed separately. The default Privileged mode password is the same for each CLI user account. You should change the Privileged mode password to secure access to the CLI configuration options.

IMPORTANT Each vShield virtual machine has two built-in CLI user accounts for system use: nobody and vs_comm. Do not delete or modify these accounts. If these accounts are deleted or modified, the virtual machine will not work.

Add a CLI User Account

You can add a user account with a strong password to secure CLI access to each vShield virtual machine. After adding a user account, you should delete the admin user account.

To add a CLI user account

1. Log in to the vSphere Client.
2. Select a vShield virtual machine from the inventory.
3. Click the Console tab to open a CLI session.
4. Log in by using the admin account.
   
   ```
   manager login: admin
   password: 
   manager>
   ```
5. Switch to Privileged mode.
   
   ```
   manager> enable
   password: 
   manager#
   ```
6 Switch to Configuration mode.
   
   manager# configure terminal

7 Add a user account.
   
   manager(config)# user root password plaintext abcd1234

8 Save the configuration.
   
   manager(config)# write memory
   Building Configuration...
   Configuration saved.
   [OK]

9 Exit the CLI.
   
   manager(config)# exit
   manager# exit

Delete the admin User Account from the CLI

After adding a CLI user account, you can delete the admin user account to secure access to the CLI.

IMPORTANT  Do not delete the admin user account until you add a user account to replace the admin account. This prevents you from being locked out of the CLI.

To delete the admin user account
1 Log in to the vSphere Client.
2 Select a vShield virtual machine from the inventory.
3 Click the **Console** tab to open a CLI session.
4 Log in by using a user account other than admin.
5 Switch to Privileged mode.
6 Switch to Configuration mode.
7 Delete the admin user account.
   
   manager(config)# no user admin
8 Save the configuration.
9 Run the **exit** command twice to log out of the CLI.

Change the CLI Privileged Mode Password

You can change the Privileged mode password to secure access to the configuration options of the CLI.

To change the Privileged mode password
1 Log in to the vSphere Client.
2 Select a vShield virtual machine from the inventory.
3 Click the **Console** tab to open a CLI session.
4 Log in to the CLI.
5 Switch to Privileged mode.
6 Switch to Configuration mode.
7 Change the Privileged mode password.
   
   manager(config)# enable password abcd1234
8 Save the configuration.
9 Run the exit command twice to log out of the CLI.
10 Log in to the CLI.
11 Switch to Privileged mode by using the new password.

Command Reference
The command reference details each CLI command, including syntax, usage, and related commands.

- “Administrative Commands” on page 93
- “CLI Mode Commands” on page 94
- “Configuration Commands” on page 97
- “Debug Commands” on page 104
- “Show Commands” on page 109
- “Diagnostics and Troubleshooting Commands” on page 125
- “User Administration Commands” on page 128
- “Terminal Commands” on page 130
- “Deprecated Commands” on page 131

Administrative Commands

list
Lists all in-mode commands.

Syntax
list

CLI Mode
Basic, Privileged, Configuration, Interface Configuration

Example
vShieldMgr> list
  enable
  exit
  list
  ping WORD
  quit
  show interface
  show ip route
  ssh WORD
  telnet WORD
  telnet WORD PORT
  tracert WORD
  ...

reboot
Reboots a vShield virtual machine. You can also reboot a vShield App from the vShield Manager user interface. See “Restart a vShield App” on page 63.

Syntax
reboot
CLI Mode
Privileged

Example
vShield# reboot

Related Commands
shutdown

shutdown
In Privileged mode, the shutdown command powers off the virtual machine. In Interface Configuration mode, the shutdown command disables the interface.
To enable a disabled interface, use no before the command.

Syntax
[no] shutdown

CLI Mode
Privileged, Interface Configuration

Example
vShield# shutdown
or
vShield(config)# interface mgmt
vShield(config-if)# shutdown
vShield(config-if)# no shutdown

Related Commands
reboot

CLI Mode Commands

configure terminal
Switches to Configuration mode from Privileged mode.

Syntax
configure terminal

CLI Mode
Privileged

Example
vShield# configure terminal
vShield(config)#

Related Commands
interface
disable

Switches to Basic mode from Privileged mode.

Syntax
disable
## CLI Mode

### Basic

#### Example

vShield# disable
vShield>

**Related Commands**

enable

**enable**

Switches to Privileged mode from Basic mode.

#### Syntax

enable

### CLI Mode

Basic

#### Example

vShield> enable
password:
vShield#

**Related Commands**

disable

disable

#### Syntax

disable

deable

#### end

Ends the current CLI mode and switches to the previous mode.

**Syntax**

end

### CLI Mode

Basic, Privileged, Configuration, and Interface Configuration

#### Example

vShield# end
vShield>

**Related Commands**

exit

**exit**

Exits from the current mode and switches to the previous mode, or exits the CLI session if run from Privileged or Basic mode.

**Syntax**

exit

### CLI Mode

Basic, Privileged, Configuration, and Interface Configuration
Example

vShield(config-if)# exit
vShield(config)# exit
vShield#

Related Commands

end
quit

interface

Switches to Interface Configuration mode for the specified interface.
To delete the configuration of an interface, use no before the command.

Syntax

[no] interface (mgmt | p0 | u0)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>The management port on a vShield virtual machine.</td>
</tr>
<tr>
<td>p0</td>
<td>vShield App p0 interface.</td>
</tr>
<tr>
<td>u0</td>
<td>vShield App u0 interface.</td>
</tr>
</tbody>
</table>

CLI Mode

Configuration

Example

vShield# configure terminal
vShield(config)# interface mgmt
vShield(config-if)#
or
vShield(config)# no interface mgmt

Related Commands

show interface

quit

Quits Interface Configuration mode and switches to Configuration mode, or quits the CLI session if run from Privileged or Basic mode.

Syntax

quit

CLI Mode

Basic, Privileged, and Interface Configuration

Example

vShield(config-if)# quit
vShield(config)#

Related Commands

end
exit
Configuration Commands

**clear vmwall rules**
Resets the firewall rule set on a vShield App to the default rule set. This is a temporary condition that can be used to troubleshoot firewall issues. You can restore the firewall rule set by performing a force sync operation for the vShield App from the vShield Manager. For more information on forcing synchronization, see “Force a vShield App to Synchronize with the vShield Manager” on page 62.

**Syntax**
clear vmwall rules

**CLI Mode**
Privileged

**Usage Guidelines**
vShield App CLI

**Example**
manager# clear vmwall rules

**Related Commands**
show vmwall log
show vmwall rules

**cli ssh allow**
Enable or disable access to the CLI via SSH session.

**Syntax**
[no] cli ssh allow

**CLI Mode**
Configuration

**Usage Guidelines**
Use this command with the ssh command to allow or disallow CLI access via SSH.

**Example**
manager(config)# ssh start
manager(config)# cli ssh allow

**Related Commands**
ssh

**copy running-config startup-config**
Copies the current system configuration to the startup configuration. You can also copy and save the running CLI configuration of a vShield App from the vShield Manager user interface. See “Back Up the Running CLI Configuration of a vShield App” on page 62.

**Syntax**
copy running-config startup-config

**CLI Mode**
Privileged
Example

```
manager# copy running-config startup-config
Building Configuration...
Configuration saved.
[OK]
```

**Related Commands**

- `show running-config`
- `show startup-config`

**database erase**

Erases the vShield Manager database, resetting the database to factory defaults. This command clears all configuration data from the vShield Manager user interface, including vShield App configurations, event data, and so forth. The vShield Manager CLI configuration is not affected by this command.

**Syntax**

```
database erase
```

**CLI Mode**

Privileged

**Usage Guidelines**

vShield Manager CLI

**Example**

```
manager# database erase
```

**enable password**

Changes the Privileged mode password. You should change the Privileged mode password for each vShield virtual machine. CLI user passwords and the Privileged mode password are managed separately. The Privileged mode password is the same for each CLI user account.

**Syntax**

```
enable password PASSWORD
```

**Option Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td>Password to use. The default password is default.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Configuration

**Example**

```
vShield# configure terminal
vShield(config)# enable password plaintext abcd123
```

**Related Commands**

- `enable`
- `show running-config`
hostname
Changes the name of the CLI prompt. The default prompt name for the vShield Manager is manager, and the default prompt name for the vShield App is vShield.

Syntax
hostname WORD

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Prompt name to use.</td>
</tr>
</tbody>
</table>

CLI Mode
Configuration

Example
vShield(config)# hostname vs123
vs123(config)#

ip address
Assigns an IP address to an interface. On the vShield virtual machines, you can assign an IP addresses to the mgmt interface only.

To remove an IP address from an interface, use no before the command.

Syntax
[no] ip address A.B.C.D/M

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IP address to use.</td>
</tr>
<tr>
<td>M</td>
<td>Subnet mask to use.</td>
</tr>
</tbody>
</table>

CLI Mode
Interface Configuration

Example
vShield(config)# interface mgmt
vShield(config-if)# ip address 192.168.110.200/24
or
vShield(config)# interface mgmt
vShield(config-if)# no ip address 192.168.110.200/24

Related Commands
show interface

ip name server
Identifies a DNS server to provide address resolution service. You can also identify one or more DNS servers by using the vShield Manager user interface. See “Identify DNS Services” on page 22.

To remove a DNS server, use no before the command.
Syntax
[no] ip name server A.B.C.D

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IP address to use.</td>
</tr>
</tbody>
</table>

**CLI Mode**

**Configuration**

**Example**

vShield(config)# ip name server 192.168.1.3

or

vShield(config)# no ip name server 192.168.1.3

**ip route**

Adds a static route.

To delete an IP route, use no before the command.

**Syntax**

[no] ip route A.B.C.D/M W.X.Y.Z

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IP address to use.</td>
</tr>
<tr>
<td>M</td>
<td>Subnet mask to use.</td>
</tr>
<tr>
<td>W.X.Y.Z</td>
<td>IP address of network gateway.</td>
</tr>
</tbody>
</table>

**CLI Mode**

**Configuration**

**Example**

vShield# configure terminal
vShield(config)# ip route 0.0.0.0/0 192.168.1.1

or

vShield(config)# no ip route 0.0.0.0/0 192.168.1.1

**Related Commands**

show ip route

**manager key**

Sets a shared key for authenticating communication between a vShield App and the vShield Manager. You can set a shared key on any vShield App. This key must be entered during vShield App installation. If the shared key between a vShield App and the vShield Manager is not identical, the service cannot install and is inoperable.

**Syntax**

manager key KEY

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY</td>
<td>The key that the vShield App and vShield Manager must match.</td>
</tr>
</tbody>
</table>
**CLI Mode**
Privileged

**Usage Guidelines**
vShield App CLI

**Example**
vShield# manager key abc123

**Related Commands**
setup

**ntp server**
Identifies a Network Time Protocol (NTP) server for time synchronization service. Initial NTP server synchronization might take up to 15 minutes. From the vShield Manager user interface, you can connect to an NTP server for time synchronization. See “Set the vShield Manager Date and Time” on page 23.

All vShield App instances use the NTP server configuration of the vShield Manager. You can use this command to connect a vShield App to an NTP server not used by the vShield Manager.

To remove the NTP server, use no before the command.

**Syntax**
```
[no] ntp server (HOSTNAME | A.B.C.D)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>Hostname of the NTP server.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP address of NTP server.</td>
</tr>
</tbody>
</table>

**CLI Mode**
Configuration

**Usage Guidelines**
vShield App CLI

**Example**
```
vShield# configure terminal
vShield(config)# ntp server 10.1.1.113
```

or
```
vShield# configure terminal
vShield(config)# no ntp server
```

**Related Commands**
show ntp

**set clock**
Sets the date and time. From the vShield Manager user interface, you can connect to an NTP server for time synchronization. All vShield App instances use the NTP server configuration of the vShield Manager. You should use this command if you meet one of the following conditions.

- You cannot connect to an NTP server.
- You frequently power off and power on a vShield App, such as in a lab environment. A vShield App can become out of sync with the vShield Manager when it is frequently power on and off.
Syntax

```
set clock HH:MM:SS MM DD YYYY
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH:MM:SS</td>
<td>Hours:minutes:seconds</td>
</tr>
<tr>
<td>MM</td>
<td>Month</td>
</tr>
<tr>
<td>DD</td>
<td>Day</td>
</tr>
<tr>
<td>YYYY</td>
<td>Year</td>
</tr>
</tbody>
</table>

CLI Mode

Privileged

Example

```
vShield(config)# set clock 00:00:00 08 28 2009
```

Related Commands

- `ntp server`
- `show clock`
- `show ntp`

**setup**

Opens the CLI initialization wizard for vShield virtual machine installation. You configure multiple settings by using this command. You run the `setup` command during vShield Manager installation and manual installation of vShield App instances. Press ENTER to accept a default value.

Syntax

```
setup
```

CLI Mode

Basic

Usage Guidelines

The `Manager` key option is applicable to vShield App setup only.

Example

```
manager(config)# setup
Default settings are in square brackets '[]'.
Hostname [manager]:
IP Address (A.B.C.D or A.B.C.D/MASK): 192.168.0.253
Default gateway (A.B.C.D): 192.168.0.1
Old configuration will be lost, and system needs to be rebooted
Do you want to save new configuration (y/[n]): y
Please log out and log back in again.
```

manager>

**ssh**

Starts or stops the SSH service on a vShield virtual appliance.

Syntax

```
ssh (start | stop)
```
**CLI Mode**
Configuration

**Usage Guidelines**
Starting the SSH service and enabling CLI access via SSH (cli ssh allow) allows user to access the CLI via SSH.

**Example**
manager(config)# ssh start
manager(config)# cli ssh allow

or

manager(config)# no cli ssh allow
manager(config)# ssh stop

**Related Commands**
cli ssh allow

**syslog**
Identifies a syslog server to which a vShield virtual machine can send system events. You can also identify one or more syslog servers by using the vShield Manager user interface. See “Send vShield App System Events to a Syslog Server” on page 61.

To disable syslog export, use no before the command.

**Syntax**

```
[no] syslog (HOSTNAME | A.B.C.D)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>Hostname of the syslog server.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP address of syslog server.</td>
</tr>
</tbody>
</table>

**CLI Mode**
Configuration

**Example**

```
vShield(config)# syslog 192.168.1.2
```

**Related Commands**

show syslog

**write**
Writes the running configuration to memory. This command performs the same operation as the `write memory` command.

**Syntax**

```
write
```

**CLI Mode**
Privileged

**Example**

```
manager# write
```
### Related Commands

**write memory**

**write erase**
Resets the CLI configuration to factory default settings.

**Syntax**

`write erase`

**CLI Mode**

Privileged

**Example**

`manager# write erase`

**write memory**
Writes the current configuration to memory. This command is identical to the `write` command.

**Syntax**

`write memory`

**CLI Mode**

Privileged, Configuration, and Interface Configuration

**Example**

`manager# write memory`

### Related Commands

`write`

### Debug Commands

**debug copy**
Copies one or all packet trace or tcpdump files and exports them to a remote server. You must enable the `debug packet capture` command before you can copy and export files.

**Syntax**

```
debug copy (scp|ftp) URL (packet-traces | tcpdumps) (FILENAME | all)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scp</td>
<td>Use SCP as transport protocol.</td>
</tr>
<tr>
<td>ftp</td>
<td>Use FTP as transport protocol.</td>
</tr>
<tr>
<td>URL</td>
<td>Add a URL in the format user@&lt;ip_address&gt;:&lt;directory&gt;. For example: admin@10.10.1.10:/tmp</td>
</tr>
<tr>
<td>packet-traces</td>
<td>Copy and export packet traces.</td>
</tr>
<tr>
<td>tcpdumps</td>
<td>Copy and export system tcpdumps.</td>
</tr>
<tr>
<td>FILENAME</td>
<td>Identify a specific packet trace or tcpdump file to export.</td>
</tr>
<tr>
<td>all</td>
<td>Copy and export all packet trace or tcpdump files.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Privileged
Usage Guidelines
vShield App CLI

Example
vShield# debug copy ftp 192.168.1.1 tcpdumps all

Related Commands
dbg packet capture
dbg remove
dbg show files

dbg packet capture
Captures all packets processed by a vShield App, similar to a tcpdump. Enabling this command can slow vShield App performance. Packet debug capture is disabled by default.

To disable packet capture, use no before the command.

Syntax
[no] debug packet capture (segment 0 | interface (mgmt | u0 | p0)) [EXPRESSION]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>segment 0</td>
<td>The segment on the vShield App for which the debug function captures tcpdump information. Segment 0 is the only active segment. Segments 1 and 2 have been deprecated.</td>
</tr>
<tr>
<td>interface (mgmt</td>
<td>u0</td>
</tr>
<tr>
<td>EXPRESSION</td>
<td>A tcpdump-formatted string. You must use an underscore between words in the expression.</td>
</tr>
</tbody>
</table>

CLI Mode
Privileged

Usage Guidelines
vShield App CLI

Example
vShield# debug packet capture segment 0 host_10.10.11.11_port_8

Related Commands
dbg copy
dbg packet display interface

dbg packet display interface
Displays all packets captured by a vShield App or vShield Edge interface, similar to a tcpdump. Enabling this command can impact vShield App or vShield Edge performance.

To disable the display of packets, use no before the command.
Syntax

vShield App

[no] debug packet display interface (mgmt | u0 | p0) [EXPRESSION]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>u0</td>
</tr>
<tr>
<td>EXPRESSION</td>
<td>A tcpdump-formatted string. You must use an underscore between words in the expression.</td>
</tr>
</tbody>
</table>

vShield Edge

[no] debug packet display interface (intif | extif) [EXPRESSION]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>intif</td>
<td>extif</td>
</tr>
<tr>
<td>EXPRESSION</td>
<td>A tcpdump-formatted string. You must use an underscore between words in the expression.</td>
</tr>
</tbody>
</table>

CLI Mode

Privileged

Usage Guidelines

vShield App or vShield Edge CLI

Example

vShield# debug packet display interface mgmt host_10.10.11.11_and_port_80

Related Commands

dump packet capture

dump remove

Removes one or all packet trace or tcpdump files from a vShield App.

Syntax

dump remove (packet-traces|tcpdumps) (FILENAME | all)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet-traces</td>
<td>Remove one or all packet trace files.</td>
</tr>
<tr>
<td>tcpdumps</td>
<td>Remove one or all tcpdump files.</td>
</tr>
<tr>
<td>FILENAME</td>
<td>Identify a specific packet trace or tcpdump file to export.</td>
</tr>
<tr>
<td>all</td>
<td>Remove all packet trace or tcpdump files.</td>
</tr>
</tbody>
</table>

CLI Mode

Privileged

Usage Guidelines

vShield App CLI

Example

vShield# dump remove tcpdumps all
Related Commands

- debug copy
- debug packet capture
- debug show files
- debug service

**debug service**

Enables logging for a service, noting the specific engine for the service and the severity of events to log. You can run the `show services` command to view the list of running services.

To disable logging for a specific service, use `no` before the command.

**Syntax**

```
[no] debug SERVICE (ice|sysmgr|vdb|WORD) (low|medium|high)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVICE</td>
<td>Name of the service.</td>
</tr>
<tr>
<td>ice</td>
<td>vShield App protocol decoding engine.</td>
</tr>
<tr>
<td>sysmgr</td>
<td>vShield App system manager.</td>
</tr>
<tr>
<td>vdb</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>WORD</td>
<td>Reserved for technical support.</td>
</tr>
<tr>
<td>low</td>
<td>Low severity events.</td>
</tr>
<tr>
<td>medium</td>
<td>Medium severity events.</td>
</tr>
<tr>
<td>high</td>
<td>High severity events.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Privileged

**Usage Guidelines**

vShield App CLI

**Example**

```
vShield# debug 2050001_SAFLOW-FTPD-Dynamic-Port-Detection sysmgr high
```

**Related Commands**

- show services
- debug service flow src

**debug service flow src**

Debugs messages for a service that is processing traffic between a specific source-to-destination pair. You can run the `show services` command to view the list of running services.

To disable logging, use `no` before the command.

**Syntax**

```
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVICE</td>
<td>The name of the service.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Source IP address to use.</td>
</tr>
<tr>
<td>M</td>
<td>Source subnet mask to use.</td>
</tr>
<tr>
<td>P</td>
<td>Source port to use.</td>
</tr>
</tbody>
</table>
CLI Mode

Privileged

Usage Guidelines

vShield App CLI. A source or destination value of 0.0.0.0/0:0 matches all values.

Example

vShield# debug 2050001_SAFLLOW-FTPD-Dynamic-Port-Detection src 192.168.110.199/24:1234 dst 192.168.110.200/24:4567

Related Commands

show services

debug show files

Shows the tcpdump files that have been saved.

Syntax

depbug show files

CLI Mode

Privileged

Usage Guidelines

vShield App CLI

Example

vShield_Zones_host_49_269700# debug show files
total 0
-rw-r--r-- 1 0 Jun 23 16:04 tcpdump.d0.0

Related Commands

depbug copy
depbug remove
Show Commands

**show alerts**

Shows system alerts as they relate to the protocol decoders or network events. If no alerts have been raised, no output is returned.

**Syntax**

```plaintext
show alerts (vulnerability|decoder|events)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vulnerability</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>decoder</td>
<td>Alerts raised by protocol decoder errors.</td>
</tr>
<tr>
<td>events</td>
<td>Alerts raised by network events.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield App CLI

**Example**

```plaintext
vShield# show alerts events
IP address       HW type     Flags       HW address            Mask     Device
192.0.2.130      0x1         0x6         00:00:00:00:00:81     *        virteth1
192.168.110.1    0x1         0x2         00:0F:90:D5:36:C1     *        mgmt
```

**show arp**

Shows the contents of the ARP cache.

**Syntax**

```plaintext
show arp
```

**CLI Mode**

Basic, Privileged

**Example**

```plaintext
vShield# show arp
IP address       HW type     Flags       HW address            Mask     Device
192.0.2.130      0x1         0x6         00:00:00:00:00:81     *        virteth1
192.168.110.1    0x1         0x2         00:0F:90:D5:36:C1     *        mgmt
```

**show clock**

Shows the current time and date of the virtual machine. If you use an NTP server for time synchronization, the time is based on Coordinated Universal Time (UTC).

**Syntax**

```plaintext
show clock
```

**CLI Mode**

Basic, Privileged

**Example**

```plaintext
vShield# show clock
Wed Feb  9 13:04:50 UTC 2005
```
vShield Administration Guide

Related Commands

ntp server
set clock

show configuration

Shows either the current global configuration or the configuration for a specified service on a vShield Edge.

Syntax

show configuration (dhcp | firewall | ipsec | lb | nat | syslog | system)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>Show the current DHCP configuration.</td>
</tr>
<tr>
<td>firewall</td>
<td>Show the current firewall configuration.</td>
</tr>
<tr>
<td>ipsec</td>
<td>Show the current VPN configuration.</td>
</tr>
<tr>
<td>lb</td>
<td>Show the current Load Balancer configuration.</td>
</tr>
<tr>
<td>nat</td>
<td>Show the current NAT configuration.</td>
</tr>
<tr>
<td>syslog</td>
<td>Show the current syslog configuration.</td>
</tr>
<tr>
<td>system</td>
<td>Show the current global configuration.</td>
</tr>
</tbody>
</table>

CLI Mode

Basic, Privileged

Usage Guidelines

vShield Edge CLI

Example

vShieldEdge# show configuration system

show debug

Show the debug processes that are enabled. You must enable a debug path by running the debug packet or one of the debug service commands.

Syntax

show debug

CLI Mode

Basic, Privileged

Usage Guidelines

vShield App CLI

Example

vShield# show debug
No debug logs enabled

Related Commands

d debug service
d debug service flow src
**show ethernet**

Shows Ethernet information for virtual machine interfaces.

**Syntax**

`show ethernet`

**CLI Mode**

Basic, Privileged

**Example**

```
vShield# show ethernet
Settings for mgmt:
  Supported ports: [ TP ]
  Supported link modes: 10baseT/Half 10baseT/Full
  100baseT/Half 100baseT/Full
  1000baseT/Full
  Supports auto-negotiation: Yes
  Advertised link modes: 10baseT/Half 10baseT/Full
  100baseT/Half 100baseT/Full
  1000baseT/Full
  Advertised auto-negotiation: Yes
  Speed: 100Mb/s
  Duplex: Full
```

**show filesystem**

Shows the hard disk drive capacity for a vShield virtual machine. vShield App instances have one disk drive; the vShield Manager has two disk drives.

**Syntax**

`show filesystem`

**CLI Mode**

Basic, Privileged

**Example**

```
vShield# show filesystem
Filesystem            Size  Used  Avail  Use% Mounted on
/dev/hda3             4.9G   730M  3.9G  16%  /
/dev/hda6             985M   17M  919M   2%  /tmp
/dev/hda7              24G  1.7G  21G   8%  /common
```

**show gateway rules**

Shows the current IP rules running on the vShield App.

**Syntax**

`show gateway rules`

**CLI Mode**

Privileged

**Example**

```
vShield# show gateway rules
bufsz:8192 inadequate for all rules; new bufsize = 9980
size of rule_details = 36
Kernel Rules Begin

  Proxy Id = 0, Service Name = proxy-unused, Num Threads = 0 ACTION=FORWARD
  Proxy Id = 1, Service Name = proxy-zombie, Num Threads = 0 ACTION=FORWARD
```
Proxy Id = 2, Service Name = vproxy-forward-allow, Num Threads = 0 ACTION=VPROXY
Proxy Id = 3, Service Name = vproxy-reverse-allow, Num Threads = 0 ACTION=UNKNOWN

show hardware
Shows the components of the vShield virtual machine.

Syntax
show hardware

CLI Mode
Basic, Privileged

Example
manager# show hardware
-0000:00-++00.0  Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge
++01.0-[0000:01]----
++07.0  Intel Corporation 82371AB/EB/MB PIIX4 ISA
++07.1  Intel Corporation 82371AB/EB/MB PIIX4 IDE
++07.3  Intel Corporation 82371AB/EB/MB PIIX4 ACPI
++07.7  VMware Inc Virtual Machine Communication Interface
++0f.0  VMware Inc Abstract SVGA II Adapter
++10.0  BusLogic BT-946C (BA80C30) [MultiMaster 10]
++11.0-[0000:02]----00.0  Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
++15.0-[0000:03]---
...

show hostname
Shows the current hostname for a vShield Edge.

Syntax
show hostname

CLI Mode
Basic, Privileged

Usage Guidelines
vShield Edge CLI

Example
vshieldEdge# show hostname

show interface
Shows the status and configuration for all interfaces or a single interface. You can also view interface statistics for a vShield App from the vShield Manager user interface. See “View the Current System Status of a vShield App” on page 62.
Syntax

show interface [mgmt | p0 | u0]

Option | Description
--- | ---
mgmt | Management interface
p0 | vShield App P0 interface
u0 | vShield App port U0 interface

CLI Mode

Basic, Privileged

Example

manager# show interface mgmt
Interface mgmt is up, line protocol is up
  index 1 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:9e:7a:60
  inet 10.115.216.63/22 broadcast 10.115.219.255
  Auto-duplex (Full), Auto-speed (1000Mb/s)
  input packets 5492438, bytes 2147483647, dropped 0, multicast packets 0
  input errors 0, length 0, overrun 0, CRC 0, fifo 0, missed 0
  output packets 2754582, bytes 559149291, dropped 0
  output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0

Related Commands

interface

show ip addr

Shows the protocol addresses configured on a vShield Edge for all devices.

Syntax

show ip addr

CLI Mode

Basic, Privileged

Example

vShield# show ip addr

show ip route

Shows the IP routing table.

Syntax

show ip route [A.B.C.D/M]

Option | Description
--- | ---
A.B.C.D | IP address to use.
M | Subnet mask to use.

CLI Mode

Basic, Privileged
Example

vShield# show ip route
Codes: K - kernel route, C - connected, S - static,
> - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.110.1, mgmt
C>* 192.168.110.0/24 is directly connected, mgmt

Related Commands

ip route

show iptables

Shows the IP routing table.

Syntax

show iptables [filter | mangle | nat | raw]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Show the packet filtering table.</td>
</tr>
<tr>
<td>mangle</td>
<td>Show the mangle table. The mangle table is responsible for modification of the TCP packet QoS bits before routing occurs.</td>
</tr>
<tr>
<td>nat</td>
<td>Show the NAT table. NAT facilitates the transformation of the destination IP address to be compatible with the firewall’s routing table.</td>
</tr>
<tr>
<td>raw</td>
<td>Show the raw table. The raw table is used to set a mark on packets that should not be handled by the connection tracking system.</td>
</tr>
</tbody>
</table>

CLI Mode

Basic, Privileged

Example

vShield# show iptables

show kernel message

Shows the last 10 kernel messages for a vShield Edge.

Syntax

show kernel message

CLI Mode

Basic, Privileged

Usage Guidelines

vShield Edge CLI

Example

vshieldEdge# show kernel message

Related Commands

show kernel message last
show kernel message last
Shows last \( n \) kernel messages for a vShield Edge.

**Syntax**

show kernel message last \( n \)

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield Edge CLI

**Example**

vshieldEdge# show kernel message last 20

**Related Commands**

show kernel message

**show log**

Shows the system log.

**Syntax**

show log [follow | reverse]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>follow</td>
<td>Update the displayed log every 5 seconds.</td>
</tr>
<tr>
<td>reverse</td>
<td>Show the log in reverse chronological order.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic, Privileged

**Example**

vShield# show log
Aug 7 17:32:37 vShield_118 syslog-ng[27397]: Configuration reload request received, reloading configuration;
Aug 7 17:32:37 vShield_118 udev[21427]: removing device node '/dev/vcs12'
Aug 7 17:32:37 vShield_118 udev[21429]: removing device node '/dev/vcsa12'
Aug 7 17:32:37 vShield_118 udev[21432]: creating device node '/dev/vcs12'
Aug 7 17:32:37 vShield_118 udev[21433]: creating device node '/dev/vcsa12'
Aug 7 17:33:37 vShield_118 ntpdate[21445]: adjust time server 10.115.216.84 offset 0.011031 sec
Aug 7 17:34:37 vShield_118 ntpdate[21446]: adjust time server 10.115.216.84 offset 0.002739 sec
Aug 7 17:35:37 vShield_118 ntpdate[21483]: adjust time server 10.115.216.84 offset 0.010884 sec
...

**Related Commands**

show log alerts
show log events
show log last

**show log alerts**

Shows the log of firewall rule alerts.

**Syntax**

show log alerts
**CLI Mode**
Basic, Privileged

**Usage Guidelines**
vShield App CLI

**Example**
vShield# show log alerts

**Related Commands**
show log

**show log events**
Shows the log of vShield App system events.

**Syntax**
show log events

**CLI Mode**
Basic, Privileged

**Usage Guidelines**
vShield App CLI

**Example**
vShield# show log events

**Related Commands**
show log

**show log last**
Shows last n lines of the log.

**Syntax**
show log last NUM

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUM</td>
<td>Number of log lines to display</td>
</tr>
</tbody>
</table>

**CLI Mode**
Basic, Privileged

**Example**
vShield# show log last 2
Feb  9 12:30:55 localhost ntpdate[24503]: adjust time server 192.168.110.199 off set -0.000406 sec
Feb  9 12:31:54 localhost ntpdate[24580]: adjust time server 192.168.110.199 off set -0.000487 sec

**Related Commands**
show log
**show manager log**
Shows the system log of the vShield Manager.

**Syntax**
show manager log [follow | reverse]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>follow</td>
<td>Update the displayed log every 5 seconds.</td>
</tr>
<tr>
<td>reverse</td>
<td>Show the log in reverse chronological order.</td>
</tr>
</tbody>
</table>

**CLI Mode**
Basic, Privileged

**Usage Guidelines**
vShield Manager CLI

**Example**
vShield# show manager log
SEM Debug Nov 15, 2005 02:46:23 PM PropertyUtils Prefix:applicationDir
SEM Debug Nov 15, 2005 02:46:23 PM PropertyUtils Props Read:[]
SEM Info Nov 15, 2005 02:46:23 PM RefreshDb UpdateVersionNumbers info does not exist
SEM Debug Nov 15, 2005 02:46:23 PM RefreshDb Applications: []
SEM Info Nov 15, 2005 02:46:23 PM RefreshDb Compiler version pairs found: []

**Related Commands**
show manager log last

**show manager log last**
Shows the last n number of events in the vShield Manager log.

**Syntax**
show manager log last NUM

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUM</td>
<td>Number of events to display.</td>
</tr>
</tbody>
</table>

**CLI Mode**
Basic, Privileged

**Usage Guidelines**
vShield Manager CLI

**Example**
manager# show manager log last 10

**Related Commands**
show manager log

**show ntp**
Shows the IP address of the network time protocol (NTP) server. You set the NTP server IP address by using the vShield Manager user interface.
Syntax
show ntp

CLI Mode
Basic, Privileged

Usage Guidelines
vShield Manager CLI

Example
manager# show ntp
NTP server: 192.168.110.199

Related Commands
ntp server

show process
Shows information related to vShield Edge processes.

Syntax
show process (list | monitor)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>List all currently running processes on the vShield Edge.</td>
</tr>
<tr>
<td>monitor</td>
<td>Continuously monitor the list of processes.</td>
</tr>
</tbody>
</table>

CLI Mode
Basic, Privileged

Usage Guidelines
vShield Edge CLI

Example
vShieldEdge# show process list

show route
Shows the current routes configured on a vShield Edge.

Syntax
show route

CLI Mode
Basic, Privileged

Usage Guidelines
vShield Edge CLI

Example
vShieldEdge# show route

show running-config
Shows the current running configuration.
Syntax
show running-config

CLI Mode
Basic, Privileged

Example
vShield# show running-config
Building configuration...

Current configuration:
!
segment 0 default bypass
!

Related Commands
copy running-config startup-config
show startup-config

show service
Shows the status of the specified vShield Edge service.

Syntax
show service (dhcp | ipsec | lb)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>Show the status of the DHCP service.</td>
</tr>
<tr>
<td>ipsec</td>
<td>Show the status of the VPN service.</td>
</tr>
<tr>
<td>lb</td>
<td>Show the status of the Load Balancer service.</td>
</tr>
</tbody>
</table>

CLI Mode
Basic, Privileged

Usage Guidelines
vShield Edge CLI

Example
vShieldEdge# show service dhcp

show service statistics
Shows the current status of all services on a vShield Edge. Details include the running status for VPN and the Load Balancer, DHCP leases, and iptable entries for firewall and NAT.

Syntax
show service statistics

CLI Mode
Basic, Privileged

Usage Guidelines
vShield Edge CLI

Example
vShieldEdge# show service statistics
show services
Shows the services protected by a vShield App.

Syntax
show services

CLI Mode
Basic, Privileged

Usage Guidelines
vShield App CLI. In the example, 2050001_SAFLow-FTPD-Dynamic-Port-Detection is the full name of a service. You must copy and paste this string into the debug service command as the service name.

Example
vShield# show services
nproxy_D_T_0001 is ACTIVE
  56 - 2050001_SAFLow-FTPD-Dynamic-Port-Detection
  57 - 2050001_SAFLow-MSRPC-Dynamic-Port-Detection
  58 - 2050001_SAFLow-ORACLE-Dynamic-Port-Detection-Reverse
  59 - 2050001_SAFLow-FTPD-Dynamic-Port-Detection-Reverse
  60 - 2050001_SAFLow-SUNRPC-Dynamic-Port-Detection
  61 - 2050001_SAFLow-MSRPC-Dynamic-Port-Detection-Reverse
  62 - 2050001_SAFLow-SUNRPC-Dynamic-Port-Detection-Reverse
  63 - 2050001_SAFLow-ORACLE-Dynamic-Port-Detection
  64 - 2050001_SAFLow-Generic-Single-Session-Inverse-Attached
  65 - 2050001_SAFLow-Generic-Single-Session-Forward-Attached

Related Commands
ddebug service
ddebug service flow src

dshow session-manager counters
Shows historical statistics on the sessions processed by a vShield App, such as the number of SYNs received, the number of re-transmitted SYNs, and so forth.

Syntax
dshow session-manager counters

CLI Mode
Basic, Privileged

Usage Guidelines
vShield App CLI

Example
vShield# show session-manager counters
sa_tcp_sockets_allocated_high_water_mark 8
sa_tcp_tw_count_high_water_mark 3
SA_TCP_STATS_OpenreqCreated 61
SA_TCP_STATSSockCreated 61
SA_TCP_STATSNewSynReceived 61
SA_TCP_STATSRetransSynReceived 0

Related Commands
dshow session-manager sessions
show session-manager sessions
Shows the current sessions in process on a vShield App.

Syntax
show session-manager sessions

CLI Mode
Basic, Privileged

Usage Guidelines
vShield App CLI

Example
vShield# show session-manager sessions
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
  tcp    0      0 0.0.0.0:2601            0.0.0.0:*               LISTEN
  tcp    0      0 0.0.0.0:7060            0.0.0.0:*               LISTEN
   V_Listen
  tcp    0      0 192.168.110.229:46132   0.0.0.0:*               LISTEN
Related Commands
show session-manager counters

show slots
Shows the software images on the slots of a vShield virtual machine. Boot indicates the image that is used to boot the virtual machine.

Syntax
show slots

CLI Mode
Basic, Privileged

Example
manager# show slots
Recovery:  System Recovery v0.3.2
Slot 1:    13Aug09-09.49PDT
Slot 2:    * 16Aug09-23.52PDT (Boot)

show stacktrace
Shows the stack traces of failed components. If no components have failed, no output is returned.

Syntax
show stacktrace

CLI Mode
Basic, Privileged

Example
vShield# show stacktrace
**show startup-config**
Shows the startup configuration.

**Syntax**
show startup-config

**CLI Mode**
Basic, Privileged

**Example**
vShield# show startup-config

**Related Commands**
copy running-config startup-config
show running-config

**show syslog**
Shows the syslog configuration.

**Syntax**
show syslog

**CLI Mode**
Basic, Privileged

**Example**
vShield# show syslog

**Related Commands**
syslog

**show system events**
Shows the latest vShield Edge system events which have not yet been read by the vShield Manager.

**Syntax**
show system events [follow | reverse]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>follow</td>
<td>Update the displayed log every 5 seconds.</td>
</tr>
<tr>
<td>reverse</td>
<td>Show the log in reverse chronological order.</td>
</tr>
</tbody>
</table>

**CLI Mode**
Basic, Privileged

**Usage Guidelines**
vShield Edge CLI

**Example**
vShieldEdge# show system events
**show system load**
Shows the average processing load on a vShield Edge.

**Syntax**

```
show system memory
```

**CLI Mode**
Basic, Privileged

**Usage Guidelines**

vShield Edge CLI

**Example**

```
vShield# show system mem
MemTotal:   2072204 kB
MemFree:    1667248 kB
Buffers:    83120 kB
```

**show system memory**
Shows the summary of memory utilization.

**Syntax**

```
show system memory
```

**CLI Mode**
Basic, Privileged

**Example**

```
vShield# show system mem
MemTotal:   2072204 kB
MemFree:    1667248 kB
Buffers:    83120 kB
```

**show system network_connections**
Shows the currently opened network connections and listening interfaces for a vShield Edge.

**Syntax**

```
show system network_connections
```

**CLI Mode**
Basic, Privileged

**Usage Guidelines**

vShield Edge CLI

**Example**

```
vShield# show system network_connections
```

**show system storage**
Shows the disk usage details for a vShield Edge.

**Syntax**

```
show system storage
```
CLI Mode
Basic, Privileged

Usage Guidelines
vShield Edge CLI

Example
vShield# show system storage

show system uptime
Shows the length of time the vShield virtual machine has been operational since last reboot.

Syntax
show system uptime

CLI Mode
Basic, Privileged

Example
vShield# show system uptime
0 day(s), 8 hour(s), 50 minute(s), 26 second(s)

show version
Shows the software version currently running on the virtual machine.

Syntax
show version

CLI Mode
Basic, Privileged

Example
vShield# show version

show vmwall log
Shows the sessions that matched a firewall rule.

Syntax
show vmwall log [follow | reverse]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>follow</td>
<td>Update the displayed log every 5 seconds.</td>
</tr>
<tr>
<td>reverse</td>
<td>Show the log in reverse chronological order.</td>
</tr>
</tbody>
</table>

CLI Mode
Basic, Privileged

Usage Guidelines
vShield App CLI
Example
vShield# show vmwall log

Related Commands
show vmwall rules

show vmwall rules
Shows the firewall rules that are active on the vShield App.

Syntax
show vmwall rules

CLI Mode
Basic, Privileged

Usage Guidelines
vShield App CLI

Example
vShield# show vmwall rules
Printing VMWall Rules and IP Lists...

Related Commands
clear vmwall rules
show vmwall log

Diagnostics and Troubleshooting Commands

export tech-support scp
Exports the system diagnostics to a specific location via Secure Copy Protocol (SCP). You can also export system diagnostics for a vShield virtual machine from the vShield Manager user interface. See “Download a Technical Support Log from a Component” on page 23.

Syntax
export tech-support scp URL

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter the complete path of the destination.</td>
</tr>
</tbody>
</table>

CLI Mode
Basic and Privileged

Example
vShield# export tech-support scp user123@host123:file123

link-detect
Enables link detection for an interface. Link detection checks the status of an interface as enabled or disabled. Link detection is enabled by default.

To disable link detection for an interface, use no before the command.

Syntax
[no] link-detect
**CLI Mode**

Interface Configuration

**Example**

vShield(config-if)# link-detect

or

vShield(config-if)# no link-detect

**ping**

Pings a destination by its hostname or IP address.

**Syntax**

```
ping (HOSTNAME | A.B.C.D)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>A.B.C.D</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

Enter CTRL+C to end ping replies.

**Example**

vShield# ping 192.168.1.1

**ping interface addr**

Pings an external destination from the internal address of a virtual machine protected by a vShield Edge.

**Syntax**

```
ping interface addr (SOURCE_HOSTNAME | A.B.C.D) (DEST_HOSTNAME | A.B.C.D)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE_HOSTNAME</td>
<td>A.B.C.D</td>
</tr>
<tr>
<td>DEST HOSTNAME</td>
<td>A.B.C.D</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield Edge only

This command is useful for debugging IPSec-related issues.

Enter CTRL+C to end ping replies.

**Example**

vshieldEdge# ping interface addr 192.168.1.1 69.147.76.15
show tech support

Shows the system diagnostic log that can be sent to technical support by running the export tech-support scp command.

Syntax

show tech support

CLI Mode

Basic, Privileged

Example

vShield# show tech support

Related Commands

export tech-support scp

ssh

Opens an SSH connection to a remote system.

Syntax

ssh (HOSTNAME | A.B.C.D)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>The hostname or IP address of the target system.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td></td>
</tr>
</tbody>
</table>

CLI Mode

Basic, Privileged

Example

vShield# ssh server123

telnet

Opens a telnet session to a remote system.

Syntax

telnet (HOSTNAME | A.B.C.D) [PORT]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>The hostname or IP address of the target system.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td></td>
</tr>
<tr>
<td>PORT</td>
<td>Listening port on remote system.</td>
</tr>
</tbody>
</table>

CLI Mode

Basic, Privileged

Example

vShield# telnet server123

or

vShield# telnet server123 1221
**traceroute**

Traces the route to a destination.

**Syntax**

```
traceroute (HOSTNAME | A.B.C.D)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>The hostname or IP address of the target system.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td></td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic, Privileged

**Example**

```
vShield# traceroute 10.16.67.118
traceroute to 10.16.67.118 (10.16.67.118), 30 hops max, 40 byte packets
1  10.115.219.253 (10.115.219.253)  128.808 ms  74.876 ms  74.554 ms
2  10.17.248.51 (10.17.248.51)  0.873 ms  0.934 ms  0.814 ms
3  10.16.101.150 (10.16.101.150)  0.890 ms  0.913 ms  0.713 ms
4  10.16.67.118 (10.16.67.118)  1.120 ms  1.054 ms  1.273 ms
```

**validate sessions**

Validates the existing sessions against the current set of firewall rules.

**Syntax**

```
validate sessions
```

**CLI Mode**

Privileged

**Usage Guidelines**

vShield App CLI

**Example**

```
vshieldApp# validate sessions
```

**User Administration Commands**

**default web-manager password**

Resets the vShield Manager user interface admin user account password to default.

**Syntax**

```
default web-manager password
```

**CLI Mode**

Privileged mode

**Usage Guidelines**

vShield Manager CLI

**Example**

```
manager# default web-manager password
Password reset
```
**user**

Adds a CLI user account. The user admin is the default user account. The CLI admin account and password are separate from the vShield Manager user interface admin account and password.

You cannot change the password for a CLI user. You must delete a user account and re-add it to change the password. If you must change a password, create a new user account to prevent CLI lockout.

**IMPORTANT** Each vShield virtual machine has two built-in CLI user accounts for system use: nobody and vs_comm. Do not delete or modify these accounts. If these accounts are deleted or modified, the virtual machine will not work.

To remove a CLI user account, use no before the command.

**Syntax**

```
[no] user USERNAME password (hash | plaintext) PASSWORD
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
<td>Login name of the user.</td>
</tr>
<tr>
<td>hash</td>
<td>Masks the password by using the MD5 hash. You can view and copy the provided MD5 hash by running the show running-config command.</td>
</tr>
<tr>
<td>plaintext</td>
<td>Keeps the password unmasked.</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Password to use.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Configuration

**Example**

```
vShield(config)# user newuser1 password plaintext abcd1234
```

or

```
vShield(config) no user newuser1
```

**web-manager**

Starts the Web service on the vShield Manager. The Web service is started after the vShield Manager is installed.

To stop the web service (HTTP daemon) on the vShield Manager, use no before the command. This command makes the vShield Manager unavailable to Web Console browser sessions.

**Syntax**

```
[no] web-manager
```

**CLI Mode**

Configuration

**Usage Guidelines**

vShield Manager CLI. You can use this command after you have run the no web-manager command to stop and then restart the HTTP services of the vShield Manager.

**Example**

```
manager(config)# no web-manager
manager(config)# web-manager
```
Terminal Commands

**clear vty**
Clears all other VTY connections to the CLI.

**Syntax**
clear vty

**CLI Mode**
Privileged

**Example**
manager# clear vty

**reset**
Resets the terminal settings to remove the current screen output and return a clean prompt.

**Syntax**
reset

**CLI Mode**
Basic, Privileged, Configuration

**Example**
manager# reset

**Related Commands**
terminal length
terminal no length

terminal length
Sets the number of rows to display at a time in the CLI terminal.

**Syntax**
terminal length <0–512>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–512</td>
<td>Enter the number of rows to display. If length is 0, no display control is performed.</td>
</tr>
</tbody>
</table>

**CLI Mode**
Privileged

**Example**
manager# terminal length 50

**Related Commands**
reset
terminal no length

terminal no length
Negates the terminal length command.
**Syntax**

terminal no length

**CLI Mode**

Privileged

**Example**

manager# terminal no length

**Related Commands**

reset
terminal length

**Deprecated Commands**

The vShield CLI contains commands that have been deprecated. The following table lists deprecated commands.

**Table A-1. Deprecated Commands**

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>close support-tunnel</td>
</tr>
<tr>
<td>copy http URL slot (1</td>
</tr>
<tr>
<td>copy http URL temp</td>
</tr>
<tr>
<td>copy scp URL slot (1</td>
</tr>
<tr>
<td>copy scp URL temp</td>
</tr>
<tr>
<td>debug export snapshot</td>
</tr>
<tr>
<td>debug import snapshot</td>
</tr>
<tr>
<td>debug snapshot list</td>
</tr>
<tr>
<td>debug snapshot remove</td>
</tr>
<tr>
<td>debug snapshot restore</td>
</tr>
<tr>
<td>duplex auto</td>
</tr>
<tr>
<td>duplex (half</td>
</tr>
<tr>
<td>ip policy-address</td>
</tr>
<tr>
<td>linkwatch interval &lt;5-60&gt;</td>
</tr>
<tr>
<td>mode policy-based-forwarding</td>
</tr>
<tr>
<td>open support-tunnel</td>
</tr>
<tr>
<td>set support key</td>
</tr>
<tr>
<td>show raid</td>
</tr>
<tr>
<td>show raid detail</td>
</tr>
</tbody>
</table>
This appendix contains configuration examples for a basic point-to-point IPSEC VPN connection between a vShield Edge and a Cisco or WatchGuard VPN on the other end.

This appendix includes the following topics.

- “Basic Scenario” on page 133
- “Terminology” on page 134
- “IKE Phase 1 and Phase 2” on page 134
- “Configuring the vShield Edge VPN Parameters” on page 135
- “Using a Cisco 2821 Integrated Services Router” on page 137
- “Using a Cisco ASA 5510” on page 139
- “Using a WatchGuard Firebox X500” on page 141
- “Troubleshooting” on page 141

**Basic Scenario**

For this scenario, the vShield Edge connects the internal network 192.168.5.0/24 to the Internet. The vShield Edge interfaces are configured as follows:

- External Interface: 10.115.199.103
- Internal Interface: 192.168.5.1

The remote gateway connects the 172.16.0.0/16 internal network to the Internet. The remote gateway interfaces are configured as follows:

- External Interface: 10.24.120.90/24
- Internal Interface: 172.16.0.1/16

**Figure B-1.** vShield Edge connecting to a remote VPN gateway
NOTE  For vShield Edge to vShield Edge IPSEC tunnels, you can use this same scenarios by setting up the second vShield Edge as the remote gateway.

**Terminology**

IPSec is a framework of open standards. There are many technical terms in the logs of the vShield Edge and other VPN appliances that you can use to troubleshoot the IPSEC VPN.

- **ISAKMP** (Internet Security Association and Key Management Protocol) is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.

- **Oakley** is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.

- **IKE** (Internet Key Exchange) is a combination of ISAKMP framework and Oakley. vShield Edge provides IKEv2.

- **Diffie-Hellman (DH) key exchange** is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. VSE supports DH group 2 (1024 bits) and group 5 (1536 bits).

**IKE Phase 1 and Phase 2**

IKE is a standard method used to arrange secure, authenticated communications.

Phase 1 sets up mutual authentication of the peers, negotiates cryptographic parameters, and creates session keys. The Phase 1 parameters used by the vShield Edge are:

- Main mode
- TripleDES / AES [Configurable]
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret [Configurable]
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying
- ISAKMP aggressive mode disabled

IKE Phase 2 negotiates an IPSec tunnel by creating keying material for the IPSEC tunnel to use (either by using the IKE phase one keys as a base or by performing a new key exchange). The IKE Phase 2 parameters supported by vShield Edge are:

- TripleDES / AES [Will match the Phase 1 setting]
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between the two networks, using IPv4 subnets

The vShield Edge supports Main Mode for Phase 1 and Quick Mode for Phase 2.

The vShield Edge proposes a policy that requires PSK, 3DES/AES128, sha1, and DH Group 2/5. The peer must accept this policy; otherwise, the negotiation phase fails.

This example shows an exchange of Phase 1 negotiation initiated from a vShield Edge to a Cisco device.
Phase 1: Main Mode Transactions

The following transactions occur in sequence between the vShield Edge and a Cisco VPN device in Main Mode.

1. vShield Edge to Cisco
   - proposal: encrypt 3des-cbc, sha, psk, group5(group2)
   - DPD enabled

2. Cisco to vShield Edge
   - contains proposal chosen by Cisco
   - If the Cisco device does not accept any of the parameters the vShield Edge sent in step one, the Cisco device sends the message with flag NO_PROPOSAL_CHOSEN and terminates the negotiation.

3. vShield Edge to Cisco
   - DH key and nonce

4. Cisco to vShield Edge
   - DH key and nonce

5. vShield Edge to Cisco (Encrypted)
   - include ID (PSK)

6. Cisco to vShield Edge (Encrypted)
   - include ID (PSK)
   - If the Cisco device finds that the PSK doesn't match, the Cisco device sends a message with flag INVALID_ID_INFORMATION; Phase 1 fails.

Phase 2: Quick Mode Transactions

The following transactions occur in sequence between the vShield Edge and a Cisco VPN device in Quick Mode.

1. vShield Edge to Cisco
   - vShield Edge proposes Phase 2 policy to the peer. For example:
     Aug 26 12:16:09 weiqing-desktop pluto[5789]: "s1-cl" #2: initiating Quick Mode
     PSK+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW {using isakmp#1 msgid:d20849ac
     proposal=3DES(3)_192-SHA1(2)_160 pfsgroup=OAKLEY_GROUP_MODP1024}

2. Cisco to vShield Edge
   - Cisco device sends back NO_PROPOSAL_CHOSEN if it does not find any matching policy for the proposal.
   - Otherwise, the Cisco device sends the set of parameters chosen.

3. vShield Edge to Cisco
   - To facilitate debugging, you can turn on IPSec logging on the vShield Edge and enable crypto debug on Cisco (debug crypto isakmp <level>)

Configuring the vShield Edge VPN Parameters

A vShield Edge supports site-to-site IPSec VPN between a vShield Edge and remote sites.

To configure VPN on a vShield Edge

1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge.
3. Click the vShield Edge tab.
4 Click the VPN link.
5 Type an External IP Address for the VPN service on the vShield Edge.
6 Type the NATed Public IP that represents the External IP Address to the external network.
7 Select the Log check box to log VPN activity.
8 Click Apply.

Next, identify a peer site.

To identify a VPN peer site

1 Under Peer Site Configuration, click Create Site.
2 Type a name to identify the site in Site Name.
3 Type the IP address of the remote gateway in Remote Endpoint IP.
4 Type the Shared Secret.
5 Type an MTU threshold.
6 Click Add.

Next, add a tunnel to connect to the site.

To identify a VPN peer tunnel

1 Under Peer Site Configuration, select the appropriate peer from the Select or create a site drop-down list.
2 Click Add Tunnel.
3 Double-click the Tunnel Name cell and type a name to identify the tunnel.
4 Double-click the Remote Site Subnet cell and enter the IP address in CIDR format (A.B.C.D/M).
5 Double-click the Encryption cell and select the appropriate encryption type.
6 Click Commit.

Next, enable VPN service.

To enable VPN service on a vShield Edge
1 In the vSphere Client, go to Inventory > Networking.
2 Select an internal port group that is protected by a vShield Edge.
3 Click the vShield Edge tab.
4 Click the Status link.
5 Under Edge Services, select VPN and click Start to start the service.
6 If the service has been started but is not responding, click Refresh Status to send a synchronization request from the vShield Manager to the vShield Edge.

Using a Cisco 2821 Integrated Services Router

The following configurations were performed by using Cisco IOS.

Configure Interfaces and Default Route

```
interface GigabitEthernet0/0
  ip address 10.24.120.90 255.255.252.0
duplex auto
  speed auto
crypto map MYVPN
  !
interface GigabitEthernet0/1
  ip address 172.16.0.1 255.255.0.0
duplex auto
  speed auto
  !
  ip route 0.0.0.0 0.0.0.0 10.24.123.253
```

Configure IKE Policy

```
Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
```
Match Each Peer with Its Pre-Shared Secret

```
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# exit
```

Define the IPSEC Transform

```
Router# config term
Router(config)# crypto isakmp key vshield address 10.115.199.103
Router(config-isakmp)# exit
```

Create the IPSEC Access List

```
Router# config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# access-list 101 permit ip 172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit
```

Bind the Policy with a Crypto Map and Label It

In the following example, the crypto map is labeled MYVPN.

```
Router# config term
Router(config)# crypto map MYVPN 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.
Router(config-crypto-map)# set transform-set myset
Router(config-crypto-map)# set pfs group1
Router(config-crypto-map)# set peer 10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
```

Bind the Crypto Map to the Outgoing Interface

```
Router# config term
Router(config)# interface gi0/0
Router(config-if)# crypto map MYVPN
Router(config-if)# ^Z
```

Example Configuration

```
router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
```
resource policy
!
ip subnet-zero
!
ip cef
no ip dhcp use vrf connected
!
no ip ips deny-action ips-interface
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
  set peer 10.115.199.103
  set transform-set myset
  set pfs group1
  match address 101
!
interface GigabitEthernet0/0
  ip address 10.24.120.90 255.255.252.0
duplex auto
  speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
  ip address 172.16.0.1 255.255.0.0
duplex auto
  speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
  line vty 0 4
    password cisco
login
line vty 5 15
  password cisco
login
!
scheduler allocate 20000 1000
!
end

Using a Cisco ASA 5510

You can use the following output to configure a Cisco ASA 5510.

ciscoasa# show running-config output
: Saved
:
ASA Version 8.2(1)18
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted

names

! interface Ethernet0/0
 nameif untrusted
 security-level 100
 ip address 10.24.120.90 255.255.252.0
 !
 interface Ethernet0/1
 nameif trusted
 security-level 90
 ip address 172.16.0.1 255.255.0.0
 !
 interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
 !
 interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
 !
 interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 !

boot system disk0:/asa821-18-k8.bin
ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0 192.168.5.0 255.255.255.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.255.0 172.16.0.0 255.255.255.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mcp 0:05:00 mcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map MVVPN 1 match address ACL1
crypto map MVVPN 1 set pfs
crypto map MVVPN 1 set peer 10.115.199.103
crypto map MVVPN 1 set transform-set MYSET
crypto map MYVPN interface untrusted
crypto isakmp enable untrusted
crypto isakmp policy 1
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
telnet 10.0.0.0 255.0.0.0 untrusted
telnet timeout 5
ssh timeout 5
console timeout 0
no threat-detection basic-threat
no threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 10.115.199.103 type ipsec-l2l
tunnel-group 10.115.199.103 ipsec-attributes
  pre-shared-key *
!
!
prompt hostname context

Cryptochecksum:29c3cc49460831ff6c070671098085a9
: end

Using a WatchGuard Firebox X500

You can configure your WatchGuard Firebox X500 as a remote gateway.

**NOTE** Refer to your WatchGuard Firebox documentation for exact steps.

**To configure your WatchGuard Firebox X500**

1. In the Firebox System Manager, go to Tools > Policy Manager.
2. In the Policy Manager, go to Network > Configuration.
3. Configure the interfaces and click OK.
4. (Optional) Go to Network > Routes to configure a default route.
5. Go to Network > Branch Office VPN > Manual IPSec to configure the remote gateway.
6. In the IPSec Configuration dialog box, click Gateways to configure the IPSec Remote Gateway.
7. In the IPSec Configuration dialog box, click Tunnels to configure a tunnel.
8. In the IPSec Configuration dialog box, click Add to add a routing policy.
9. Close the IPSec Configuration dialog box.
10. Confirm the tunnel is up

**Troubleshooting**

**Successful Negotiation (both Phase 1 and Phase 2)**

**vShield Edge**

From the vShield Edge command line interface (ipsec auto -status, part of show service ipsec command):

000 #2: "s1-c1":500 STATE QUICK_I2 (sent QI2, IPSec SA established); EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle; import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80 tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refh1m=4294901761
Cisco

ciscoasa# show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.20.129.80
  Type : L2L       Role : responder
  Rekey : no       State : MM_ACTIVE
  Encrypt: 3des     Hash : SHA
  Auth : preshared Lifetime: 28800
  Lifetime Remaining: 28379

Phase 1 Policy Not Matching

vShield Edge

vShield Edge hangs in STATE_MAIN_I1 state. Look in /var/log/messages for information showing that, the peer sent back an IKE message with "NO_PROPOSAL_CHOSEN" set.

Aug 26 12:31:25 weiqing-desktop pluto[6569]: | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop pluto[6569]: | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop pluto[6569]: |    next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop pluto[6569]: |    length: 96
Aug 26 12:31:25 weiqing-desktop pluto[6569]: |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop pluto[6569]: |    protocol ID: 0
Aug 26 12:31:25 weiqing-desktop pluto[6569]: |    SPI size: 0
Aug 26 12:31:25 weiqing-desktop pluto[6569]: |    Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop pluto[6569]: "s1-c1" #1: ignoring informational payload, type NO_PROPOSAL_CHOSEN msgid=00000000

Cisco

If debug crypto is enabled, error message is printed to show that no proposals were accepted.

ciscoasa# Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute types for class Group
  Description: Rcv'd: Group 5  Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute types for class Group
  Description: Rcv'd: Group 5  Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + NOTIFY (11) + NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder FSM error history (struct &0x8535e060) <state>, <event>: MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA MM:9e0e4511 terminating: flags 0x01000000, refcnt 0, tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending delete/delete with reason message
Phase 2 Not Matching

vShield Edge

vShield Edge hangs at STATE_QUICK_I1. A log message shows that the peer sent a NO_PROPOSAL_CHOSEN message.

Aug 26 12:33:54 weiqing-desktop pluto[6933]: | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop pluto[6933]: | ***parse ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop pluto[6933]: |    next payload type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop pluto[6933]: |    length: 32
Aug 26 12:33:54 weiqing-desktop pluto[6933]: |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop pluto[6933]: |    protocol ID: 3
Aug 26 12:33:54 weiqing-desktop pluto[6933]: |    SPI size: 16
Aug 26 12:33:54 weiqing-desktop pluto[6933]: |    Notify Message Type: NO_PROPOSAL_CHOSEN

Cisco

Debug message show that Phase 1 is completed, but Phase 2 failed because of policy negotiation failure.

Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80, IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds.
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED Message (msgid=b2cdcb13) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0) total length : 288

Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80, Session is being torn down.
  Reason: Phase 2 Mismatch

PFS Mismatch

PFS is negotiated as part of Phase 2. If PFS does not match, the behavior is similar to the failure case described in “Phase 2 Not Matching” on page 143.

vShield Edge

Aug 26 12:35:52 weiqing-desktop pluto[7312]: | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop pluto[7312]: | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop pluto[7312]: |    next payload type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop pluto[7312]: |    length: 32
Aug 26 12:35:52 weiqing-desktop pluto[7312]: |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop pluto[7312]: |    protocol ID: 3
Aug 26 12:35:52 weiqing-desktop pluto[7312]: |    SPI size: 16
Aug 26 12:35:52 weiqing-desktop pluto[7312]: |    Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop pluto[7312]: |    Notify Message: type: NO_PROPOSAL_CHOSEN msgid=00000000
Aug 26 12:35:52 weiqing-desktop pluto[7312]: | info:  fa 16 b3 e5  91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop pluto[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop pluto[7312]: | processing informational NO_PROPOSAL_CHOSEN (14)
PSK Not Matching

PSK is negotiated in the last round of Phase 1.

vShield Edge

If PSK negotiation fails, vShield Edge state is STATE_MAIN_I4. The peer sends a message containing INVALID_ID_INFORMATION.

Packet Capture for a Successful Negotiation

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>9203</td>
<td>768.394800</td>
<td>10.20.129.80</td>
<td>10.20.131.62</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
</tbody>
</table>

Frame 9203 (190 bytes on wire, 190 bytes captured)
Internet Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
Initiator cookie: 92585D2D797E9C52
Responder cookie: 0000000000000000
Next payload: Security Association (1)
Appendix B vShield Edge VPN Configuration Examples

Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
Message ID: 0x00000000
Length: 148
Security Association payload
  Next payload: Vendor ID (13)
    Payload length: 84
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 0
      Next payload: NONE (0)
      Payload length: 72
      Proposal number: 0
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 2
      Transform payload # 0
        Next payload: Transform (3)
        Payload length: 32
        Transform number: 0
        Transform ID: KEY_IKE (1)
        Life-Type (11): Seconds (1)
        Life-Duration (12): Duration-Value (28800)
        Encryption-Algorithm (1): 3DES-CBC (5)
        Hash-Algorithm (2): SHA (2)
        Authentication-Method (3): PSK (1)
        Group-Description (4): 1536 bit MODP group (5)
      Transform payload # 1
        Next payload: NONE (0)
        Payload length: 32
        Transform number: 1
        Transform ID: KEY_IKE (1)
        Life-Type (11): Seconds (1)
        Life-Duration (12): Duration-Value (28800)
        Encryption-Algorithm (1): 3DES-CBC (5)
        Hash-Algorithm (2): SHA (2)
        Authentication-Method (3): PSK (1)
        Group-Description (4): Alternate 1024-bit MODP group (2)
    Vendor ID: 4F456C6A405D72544D42754D
      Next payload: Vendor ID (13)
      Payload length: 16
      Vendor ID: 4F456C6A405D72544D42754D
      Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
    Next payload: NONE (0)
    Payload length: 16
    Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

No.     Time        Source                Destination           Protocol Info
       9204 768.395550  10.20.131.62          10.20.129.80          ISAKMP   Identity Protection
                (Main Mode)

Frame 9204 (146 bytes on wire, 146 bytes captured)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62), Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34794CFC8CB0BD09
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 104
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 52

VMware, Inc.
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
  Next payload: NONE (0)
  Payload length: 40
  Proposal number: 1
  Protocol ID: ISAKMP (1)
  SPI Size: 0
  Proposal transforms: 1
Transform payload # 1
  Next payload: NONE (0)
  Payload length: 32
  Transform number: 1
  Transform ID: KEY_IKE (1)
  Encryption-Algorithm (1): 3DES-CBC (5)
  Hash-Algorithm (2): SHA (2)
  Group-Description (4): Alternate 1024-bit MODP group (2)
  Authentication-Method (3): PSK (1)
  Life-Type (11): Seconds (1)
  Life-Duration (12): Duration-Value (28800)
Vendor ID: Microsoft L2TP/IPSec VPN Client
Next payload: NONE (0)
Payload length: 24
Vendor ID: Microsoft L2TP/IPSec VPN Client

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>9205</td>
<td>768.399599</td>
<td>10.20.129.80</td>
<td>10.20.131.62</td>
<td>ISAKMP Identity Protection</td>
</tr>
</tbody>
</table>

(Main Mode)

Frame 9205 (222 bytes on wire, 222 bytes captured)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80), Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x000000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>9206</td>
<td>768.401192</td>
<td>10.20.131.62</td>
<td>10.20.129.80</td>
<td>ISAKMP Identity Protection</td>
</tr>
</tbody>
</table>

(Main Mode)

Frame 9206 (298 bytes on wire, 298 bytes captured)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62), Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 256
### Key Exchange payload
- **Next payload:** Nonce (10)
- **Payload length:** 132

### Nonce payload
- **Next payload:** Vendor ID (13)
- **Payload length:** 24

### Vendor ID: CISCO-UNITY-1.0
- **Next payload:** Vendor ID (13)
- **Payload length:** 20
- **Vendor ID:** CISCO-UNITY-1.0

### Vendor ID: draft-beaulieu-ike-xauth-02.txt
- **Next payload:** Vendor ID (13)
- **Payload length:** 12
- **Vendor ID:** draft-beaulieu-ike-xauth-02.txt
- **Vendor ID:** C1B7EBE18C8CBD099E89695E2CB16A4A
- **Next payload:** Vendor ID (13)
- **Payload length:** 20
- **Vendor ID:** C1B7EBE18C8CBD099E89695E2CB16A4A
- **Vendor ID:** CISCO-CONCENTRATOR
- **Next payload:** NONE (0)
- **Payload length:** 20
- **Vendor ID:** CISCO-CONCENTRATOR

| No.  | Time     | Source            | Destination        | Protocol Info
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9207</td>
<td>768.404990</td>
<td>10.20.129.80</td>
<td>10.20.131.62</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
</tbody>
</table>

Frame 9207 (110 bytes on wire, 110 bytes captured)


Internet Protocol, Src: 10.20.129.80 (10.20.129.80), Dst: 10.20.131.62 (10.20.131.62)

User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol
- Initiator cookie: 92585D2D797E9C52
- Responder cookie: 34704CFC8C8BD8D09
- Next payload: Identification (5)
- Version: 1.0
- Exchange type: Identity Protection (Main Mode) (2)
- Flags: 0x01
- Message ID: 0x00000000
- Length: 68
- Encrypted payload (40 bytes)

| No.  | Time     | Source            | Destination        | Protocol Info
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9208</td>
<td>768.405921</td>
<td>10.20.131.62</td>
<td>10.20.129.80</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
</tbody>
</table>

Frame 9208 (126 bytes on wire, 126 bytes captured)


Internet Protocol, Src: 10.20.131.62 (10.20.131.62), Dst: 10.20.129.80 (10.20.129.80)

User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol
- Initiator cookie: 92585D2D797E9C52
- Responder cookie: 34704CFC8C8BD8D09
- Next payload: Identification (5)
- Version: 1.0
- Exchange type: Identity Protection (Main Mode) (2)
- Flags: 0x01
- Message ID: 0x00000000
- Length: 84
- Encrypted payload (56 bytes)

| No.  | Time     | Source            | Destination        | Protocol Info
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9209</td>
<td>768.409799</td>
<td>10.20.129.80</td>
<td>10.20.131.62</td>
<td>ISAKMP Quick Mode</td>
</tr>
</tbody>
</table>

Frame 9209 (334 bytes on wire, 334 bytes captured)

Internet Protocol, Src: 10.20.129.80 (10.20.129.80), Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol

Initiator cookie: 92585D20797E9C52
Responder cookie: 34704CFC8C8DBD09
Next payload: Hash (8)
Version: 1.0
Exchange type: Quick Mode (32)
Flags: 0x01
Message ID: 0x79a63fb1
Length: 292

Encrypted payload (264 bytes)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>9210</td>
<td>768.411797</td>
<td>10.20.131.62</td>
<td>10.20.129.80</td>
<td>ISAKMP Quick Mode</td>
</tr>
</tbody>
</table>

Frame 9210 (334 bytes on wire, 334 bytes captured)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62), Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol

Initiator cookie: 92585D20797E9C52
Responder cookie: 34704CFC8C8DBD09
Next payload: Hash (8)
Version: 1.0
Exchange type: Quick Mode (32)
Flags: 0x01
Message ID: 0x79a63fb1
Length: 292

Encrypted payload (264 bytes)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>9211</td>
<td>768.437057</td>
<td>10.20.129.80</td>
<td>10.20.131.62</td>
<td>ISAKMP Quick Mode</td>
</tr>
</tbody>
</table>

Frame 9211 (94 bytes on wire, 94 bytes captured)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80), Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol

Initiator cookie: 92585D20797E9C52
Responder cookie: 34704CFC8C8DBD09
Next payload: Hash (8)
Version: 1.0
Exchange type: Quick Mode (32)
Flags: 0x01
Message ID: 0x79a63fb1
Length: 52

Encrypted payload (24 bytes)
Troubleshooting

This section guides you through troubleshooting common vShield issues.

This appendix covers the following topics:

- “Troubleshooting vShield Manager Installation” on page 149
- “Troubleshooting Operation Issues” on page 150
- “Troubleshooting Operation Issues” on page 150
- “Troubleshooting Port Group Isolation Issues” on page 151
- “Troubleshooting vShield Edge Issues” on page 154
- “Troubleshooting vShield Endpoint Issues” on page 155

Troubleshooting vShield Manager Installation

vShield OVA File Extracted to a PC Where vSphere Client Is Not Installed

Problem
I obtained the vShield OVA file and downloaded it to my PC. If I do not have the vSphere Client on my PC, how do I install vShield?

Solution
You must have the vSphere Client to install vShield.

vShield OVA File Cannot Be Installed in vSphere Client

Problem
When I try to install the vShield OVA file, the install fails.

Solution
If a vShield OVA file cannot be installed, an error window in the vSphere Client notes the line where the failure occurred. Send this error information with the vSphere Client build information to VMware technical support.
Cannot Log In to CLI After the vShield Manager Virtual Machine Starts

**Problem**

I cannot log in to the vShield Manager CLI after I installed the OVF.

**Solution**

Wait a few minutes after completing the vShield Manager installation to log in to the vShield Manager CLI. In the Console tab view, press Enter to check for a command prompt if the screen is blank.

Cannot Log In to the vShield Manager User Interface

**Problem**

When I try to log in to the vShield Manager user interface from my Web browser, I get a Page Not Found exception.

**Solution**

The vShield Manager IP address is in a subnet that is not reachable by the Web browser. The IP address of the vShield Manager management interface must be reachable by the Web browser to use vShield.

Troubleshooting Operation Issues

vShield Manager Cannot Communicate with a vShield App

**Problem**

I cannot configure a vShield App from the vShield Manager.

**Solution**

If you cannot configure the vShield App from the vShield Manager, there is a break in connectivity between the two virtual machines. The vShield management interface cannot talk to the vShield Manager management interface. Make sure that the management interfaces are in the same subnet. If VLANs are used, make sure that the management interfaces are in the same VLAN.

Another reason could be that the vShield App or vShield Manager virtual machine is powered off.

Cannot Configure a vShield App

**Problem**

I cannot configure a vShield App.

**Solution**

This might be the result of one of the following conditions.

- The vShield App virtual machine is corrupt. Uninstall the offending vShield App from the vShield Manager user interface. Install a new vShield App to protect the ESX host.
- The vShield Manager cannot communicate with the vShield App.
- The storage/LUN hosting the vShield configuration file has failed. When this happens, you cannot make any configuration changes. However, the firewall continues to run. You can store vShield virtual machines to local storage if remote storage is not reliable.

Take a snapshot or create a TAR of the affected vShield App by using the vSphere Client. Send this information to VMware technical support.
Firewall Block Rule Not Blocking Matching Traffic

Problem
I configured an App Firewall rule to block specific traffic. I used Flow Monitoring to view traffic, and the traffic I wanted to block is being allowed.

Solution
Check the ordering and scope of the rule. This includes the container level at which the rule is being enforced. Issues might occur when an IP address-based rule is configured under the wrong container.

Check where the affected virtual machine resides. Is the virtual machine behind a vShield App? If not, then there is no agent to enforce the rule. Select the virtual machine in the resource tree. The App Firewall tab for this virtual machine displays all of the rules that affect this virtual machine.

Place any unprotected virtual machines onto a vShield-protected switch or protect the vSwitch that the virtual machine is on by installing a vShield.

Enable logging for the App Firewall rule in question. This might slow network traffic through the vShield App.

Verify vShield App connectivity. Check for the vShield App being out of sync on the System Status page. If out of sync, click Force Sync. If it is still not in sync, go to the System Event log to determine the cause.

No Flow Data Displaying in Flow Monitoring

Problem
I have installed the vShield Manager and a vShield App. When I opened the Flow Monitoring tab, I did not see any data.

Solution
This might be the result of one or more of the following conditions.

- You did not allow enough time for the vShield App to monitor traffic sessions. Allow a few minutes after vShield App installation to collect traffic data. You can request data collection by clicking Get Latest on the Flow Monitoring tab.

- Traffic is destined to virtual machines that are not protected by a vShield App. Make sure your virtual machines are protected by a vShield App. Virtual machines must be in the same port group as the vShield App protected (p0) port.

- There is no traffic to the virtual machines protected by a vShield App.

- Check the system status of each vShield App for out-of-sync issues.

Troubleshooting Port Group Isolation Issues

Validate Installation of Port Group Isolation

To validate installation of Port Group Isolation
1. Make sure that the same port group and virtual machines are not also configured for vCloud Service Director network isolation or LabManager cross-host fencing. Double encapsulation mode is not supported currently.
2. Verify that the Port Group Isolation bundle is installed: esxupdate query
3. Verify that vshd is running.
   - ESXi: ps | grep vsh. The results might contain more than one instance, which is ok.
   - ESX Classic: ps -eo f | grep vshd
4 Verify that the kernel module is loaded: `vmkload_mod -l | grep vshd -ni`.
5 Verify that the mirror virtual machine is powered on.
   On the ESX host, look for a powered on virtual machine with `nahe vshield-infra-ni-<string>`.
6 Verify that the Port Group Isolation virtual machine is connected to the correct port group.
7 Verify that the VMX files for the protected virtual machines contain the filter entries.
   Open the VMX file and search for `filter15`. There should be three entries. Make sure these entries are present on the correct Ethernet card. Each VMX file should have only three entries per vNIC related to the fence module (filter15). If the entries are repeated, that means that the VMX file had isolation entries from a previous configuration that was not cleaned up and later duplicate entries were added.
8 Verify that all virtual machines belonging to the port group have identical filter settings in the VMX files.
9 Verify that the vshd configuration is intact.
   a Go to `/etc/opt/vmware/vsla/config`.
   b Review the files in this directory. Ensure all files contain some data. They should not be empty.

If all of the above is correct, the ESX host is set up properly for Port Group Isolation.

Verify Install or Uninstall Script

The installation script creates the following entities.

- Creates a user named `vslauser` and sets a default password.
  To see if the user was added: `vi /etc/passwd`
- Adds the role `vslauser` and associates the user `vslauser` to the role.
- Adds entries to start vshd and the script `svm-autostart` across every reboot.
  You can verify this on ESXi by looking for entries related to vshd and `svm-autostart` in the file `/etc/chkConfig.db`. On ESX, you can verify this by doing `find / -name *vsh*` and confirming that there are scripts named `S<value>vsla` and `svm-autostart`.
- Adds an entry to the services list on ESX to expose VSHD services. You can verify this entry by opening the file `/etc/vmware/hostd/proxy.xml` and searching for word `vsh`.

The removal script removes all of the operations created by the installation script.

- Removes user `vslauser`.
- Removes the role `vslauser`.
- Removes the init entries for `vshd` and `svm-autostart`.
- Removes the vshd entry from `proxy.xml`.

Validate the Data Path

**To troubleshoot packet drops, such as a ping between virtual machines in the same isolated port group**

1 Make sure that addresses, routes, netmasks, and gateways are configured correctly.
2 Install tcpdump on a virtual machine in the isolated port group.
3 Run a packet capture inside that virtual machine.
4 Ping from the problematic virtual machine to the virtual machine where captures are running.
   If an ARP packet is received, that means that broadcast packets are received. If you do not receive an ARP packet, that means none of the packets were received.
To troubleshoot if broadcast packets are being received but unicast packets are being dropped

1. Run `/opt/vmware/vslad/fence-util setSwitchMode 1` on all ESX hosts in question. This command instructs the vsdh module to broadcast all fenced packets.

   If after running the command on all hosts things start working, most of the times, this means that the issue lies with mirror virtual machines because mirror virtual machines are required to be configured correctly for the unicast packet delivery to work.

   For more on fence-util, see “Details of the fence-util Utility” on page 153.

2. On each ESX host, check the mirror virtual machine’s NICs to make sure that at least one NIC is connected to the vSwitch to which these virtual machines are connected.

3. Confirm that the filter entries for this NIC in the mirror virtual machines VMX files are correct. All of the entries for that vSwitch should have the same LanId? value.

   After fixing the problem, reset the mode to 0 by running `/opt/vmware/vslad/fence-util setSwitchMode 0`.

4. Confirm that the packets are reaching the other ESX host. If the mirror virtual machines are misconfigured, packets are dropped at the destination ESX host, not by the source host.

   If still things are not working, this would most likely mean that the unicast switching is broken somewhere on the physical boxes in the network. This is rare because if broadcast packets are reaching, that means physical connectivity is present between the virtual machines communicating with each other. If broadcast is working and unicast is not working even after putting all vsdh modules in broadcast mode using fence-utils, then problems may be present in the physical network for such unicasts.

   There is also a chance of more than one vShield Manager, Port Group Isolation, vCenter installations on the same network. In that case, some of the host key MAC addresses may get duplicated within the same physical network. Because of this, the broadcast traffic may work fine, but the unicast traffic may reach the wrong hosts because the physical switches on the network may learn about same MAC from two different places.

To troubleshoot if no packets are being received and broadcasts are being dropped

1. Confirm that the two ESX hosts are present on a common physical network and on the same VLAN.

2. In the case of legacy switches, confirm that the same port group is connected to the same named vswitch on all the ESX hosts in question.

3. Confirm that the NIC connected to these vSwitches connect to the same physical network.

4. Run `/opt/vmware/vslad/fence-util info` command multiple times on all ESX hosts to see if any dropped packet counters are incremented.

   This module also shows dropped packet numbers for unfenced packets entering into fenced vNICs. This would mean that all the other broadcasts on the network are dropped when they reach the fenced vNIC. Look for Fenced From VM and Fenced To VM counters.

5. Isolate the point where packets are getting dropped by running captures on the ESX interface at both ends.

   In cases where packets are coming out of source ESX but are not reaching the destination ESX, there are rare chances that some intelligent device in between may be dropping these packets because of an unknown eth type in the packets.

Details of the fence-util Utility

**Log Level** indicates debug log level.

**Hostkey** is the configured host ID. There is a printing mistake in the fence util program where its attaching a 0 at the end of the host id. host id of 0x30 means host Id 3.

**Configured LAN MTUs** refer to the explicitly set MTU values via vsdh.
Port ID is the first column in all other tables (Active Ports, Switch State, and Portstats). This is a unique identifier assigned by the vshd module for each fence-enabled port. This ID is internal and has no external meaning. It is the dvfilter name for that port type casted to Uint64. The port ID is useful to query values for a specific port using the fenceutil portInfo <portId> command which outputs details of only one port.

Active Ports shows all the ports/vNICs where fencing is active. This includes the mirror vNICs. Your first host has five ports enabled for fencing, two of which are mirror vNICs. The mirror vNICs can be identified by a special fence ID of fffffe. The OP1 column indicates the fence ID. In your setup, the first host has one fence with ID 000001. The next column indicates LanId? configured for that port. This is an indication of which vSwitch the ports might be connected to. In the output below, your first host has two vSwitches (legacy + dvswitches). One has been assigned LanId 1 and the other one has LanId 2. Thus, you see two mirror virtual machine vNICs (one for each vSwitch) with different LanIds in active ports.

Switch State shows the learning table of the internal unicast learning in fence module. Inner MAC means the MAC of destination VM, the outer MAC means the hostkey MAC of the host on which this VM is present. The learning builds this table by looking at packets and it tries to learn which VM is on which host. This way, when one VM on that host tries to reach another virtual machine, this table is looked up. If the destination VM’s mac is seen in the inner MAC column, then the OuterMac? is used as the destination hostkeymac to be put in the Outer MAC header added by the fence module. If an entry is not found here, such a packet will be broadcast (outer MAC header’s destination MAC will be set to broadcast). Like any other learning system, this one also has mechanisms to time out / modify learnt entries. This will take care of things like VMs moving to different hosts or to make sure that the table does not grow too much in size with stale mac entries. The used/age/seen bits represent the flags used by fence module to track frequency of these MAC entries. The learning is done on a per-port level, hence you would see the same inner MAC - outer MAC pairs on different ports. This table also shows same hostkey mac in outer MAC sections because even for VMs on the same host, the same code is used where a packet is encapsulated and sent from source port and decapsulated on the destination port. There is no optimization for same host VMs. Thus for VMs on the same host, the outer MAC will be hostkeyMAC of the same host.

Port Statistics shows packet stats on a per port basis. One port per row. The from and To vm stats indicate packets to and from vm. The subcategories indicate the specifics about the packet. The details of each counter are in the following structure. Let me know if you need any more info on this.

**Troubleshooting vShield Edge Issues**

**Virtual Machines Are Not Getting IP Addresses from the DHCP Server**

To determine why protected virtual machines are not being assigned IP addresses by a vShield Edge

1. Verify DHCP configuration was successful on the vShield Edge by running the CLI command: show configuration dhcp.
2. Check whether DHCP service is running on the vShield Edge by running CLI command: show service dhcp
3. Ensure that vmnic on virtual machine and vShield Edge is connected (vCenter > Virtual Machine > Edit Settings > Network Adapter > Connected/Connect at Power On check boxes).

When both a vShield App and vShield Edge are installed on the same ESX host, disconnection of NICs can occur if a vShield App is installed after a vShield Edge.

**Load-Balancer Does Not Work**

To determine why the load balancer service on a vShield Edge is not working

1. Verify that the Load balancer is running by running the CLI command: show service lb.

Load balancer can be started by issuing the start command.

2. Verify the load-balancer configuration by running command: show configuration lb.

This command also shows on which external interfaces the listeners are running.
Load-Balancer Throws Error 502 Bad Gateway for HTTP Requests

To determine why the load balancer service on a vShield Edge is throwing a 502 Bad Gateway error

This error occurs when the backend or Internal servers are not responding to requests.

1. Verify that internal server IP addresses are correct.
   The current configuration can be seen through the vShield Manager or through the CLI command show configuration lb.

2. Verify that internal server IP addresses are reachable from the vShield Edge internal interface.

3. Verify that internal servers are listening on the IP:Port combination specified at the time of load balancer configuration.
   If no port is specified, then IP:80 must be checked. The internal server must not listen on only 127.0.0.1:80; either 0.0.0.0:80 or <internal-ip>:80 must be open.

VPN Does Not Work

To determine why VPN does not work on a vShield Edge

1. Verify that the other endpoint of the tunnel is configured correctly. Use the CLI command: show configuration ipsec

2. Verify that IPSec service is running on the vShield Edge.
   To verify using the CLI command: show service ipsec. IPSec service has to be started by issuing the start command.
   If ipsec is running and any errors have occurred at the time of tunnel establishment, the output of show service ipsec displays relevant information.

3. Verify the configuration at both ends (vShield Edge and remoteEnd), notably the shared keys.

4. Debug MTU or fragmentation related issues by using ping with small and big packet sizes.
   - ping -s 500 ip-at-end-of-the-tunnel
   - ping -s 2000 ip-at-end-of-the-tunnel

Troubleshooting vShield Endpoint Issues

Thin Agent Logging

vShield Endpoint thin agent logging is done inside the protected virtual machines. Two registry values are read at boot time from the windows registry. They are polled again periodically.

There are two registry values, log_dest and log_level. The two entries are located in the following registry locations:

HKLM\System\CurrentControlSet\Services\VFileScsiFilter\Parameters\log_dest
HKLM\System\CurrentControlSet\Services\VFileScsiFilter\Parameters\log_level

Both are DWORD bit masks that can be any combination of the following values:

<table>
<thead>
<tr>
<th>log_dest</th>
<th></th>
<th>log_level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WINDBLOG</td>
<td>0x1</td>
<td>AUDIT</td>
<td>0x1</td>
</tr>
<tr>
<td>VMWARE_LOG</td>
<td>0x2</td>
<td>ERROR</td>
<td>0x2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WARN</td>
<td>0x4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>0x8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DEBUG</td>
<td>0x10</td>
</tr>
</tbody>
</table>
By default, the values in release builds are set to VMWARE_LOG and AUDIT.

For more on monitoring vShield Endpoint health, see Chapter 14, “vShield Endpoint Events and Alarms,” on page 81.

**Component Version Compatibility**

The SVM version and the thin agent version must be compatible.

(There will be a compatibility matrix available after 1.0 for version compatibility checking.)

To retrieve version numbers for the various components, do the following:

- **SVM:** strings libEPSec.so | grep BUILD_NUMBER provides the build number. Also, the audit logs prints the build number when libEPSec.so is initialized.

- **GVM:** Right-click on the properties of the driver files to get the build number. Also, the audit logs prints the build number (vmware.log for release).

- **vShield Endpoint Module:** The `esxupdate` command provides the installed module version. Also, the audit logs print the build number.
Index

A
accessing online help 18
adding a user 34
admin user account 34
alarms for vShield Endpoint 82
App Firewall 71
  about L4 and L2/L3 rules 72
  adding L2/L3 rules 75
  adding L4 rules 73
  adding rules from Flow Monitoring 67
  Default Rules 72
  deleting rules 77
  hierarchy of rules 72
  planning rule enforcement 72
  Revert to Snapshot 77
  validate sessions 76
Audit Logs 43, 75, 76
audit messages for vShield Endpoint 86

B
backing up the vShield Manager 24
Backup Configuration 62
Backups 24
  on-demand 39
  restoring 40
  scheduling 40
basic mode of CLI 89
block sessions 31, 51, 76

C
clear vmwall rules 97
clear vty 130
CLI
  backing up configuration 62
  configuration mode 90
  help 91
  interface mode 90
  logging in 89
  modes 89
  privileged mode 89
  syntax 90
Cluster Level Rules 28, 72
command syntax 90
configuration mode of CLI 90
configure terminal 94
connecting to vCenter Server 21
copy running-config startup-config 97
Create User 34

D
data
  on-demand backups 39
  restoring a backup 40
  scheduling backups 40
Data Center High Precedence Rules 28, 72
Data Center Low Precedence Rules 28, 72
database erase 98
date 23
date range for Flow Monitoring 66
debug copy 104
debug packet capture 105
debug packet display interface 105
debug remove 106
debug service 107
debug service flow src 107
debug show files 108
Default Policy 50
Default Rules 28, 72
default web-manager password 128
deleting a port mapping 69
deleting a user 35
DHCP 52
disable 94
DNS 22
events
  sending to syslog 61
  syslog format 42
  vShield App 42
  vShield Manager 42
events for vShield Endpoint 83
exit 95
export tech-support scp 125
F
firewall
  about 27
  add vShield Edge firewall rule 50
  adding L2/L3 rules 75
  adding L4 rules 29, 73
  adding rules from Flow Monitoring 67
  adding Zones Firewall L2/L3 rules 30
  App Firewall, about 71
  deleting rules 32, 77
  planning rule enforcement 28, 72
  Revert to Snapshot 77
  validate sessions 31, 51, 76
flow analysis date range 66
Flow Monitoring
  adding a App Firewall rule 67
  date range 66
  show report 66
Force Sync 62

G
GUI
  logging in 17
  online help 18

H
help
  CLI 91
  GUI 18
  Hide Port Mappings 69
  hierarchy of App Firewall rules 72
  hierarchy of Zones Firewall rules 28
  history of updates 38
  host alarms for vShield Endpoint 82
  hostname 99
  Hosts & Clusters view 18
  HTTP proxy 23

I
installing, updates 37
interface 96
interface mode of CLI 90
inventory panel 18
ip address 99
ip name server 99
ip route 100

L
L2/L3 rules
  about 72
  adding 30, 75
L4 rules
  about 72
  adding 29, 73
  link-detect 125
  list 93
Load Balancer 55
login
  CLI 89
  vShield Manager 17
logs
  audit 43, 75, 76
  technical support 23

M
manager key 100

N
NAT 51
Networks view 18
NTP 23
ntp server 101

O
online help 18

P
password 34
ping 126
ping interface addr 126
plug-in 22
Port Group Isolation, uninstall 46
port mappings 68
  add 68
  deleting 69
  hiding 69
privileged mode of CLI 89
proxy service 23

Q
quit 96

R
reboot 93
reports
  audit log 43, 75, 76
  system events 41
reset 130
restarting a vShield App 63
restoring backups 40
Revert to Snapshot 77
roles and rights
  about 33
  assigning to a user 34
rules
  adding L2/L3 rules to App Firewall 75
adding L2/L3 rules to Zones Firewall 30
adding L4 rules to App Firewall 73
adding L4 rules to Zones Firewall 29
deleting App Firewall rules 77
deleting Zones Firewall rules 32

S
scheduling backups 40
Secure Port Group Rules 28, 72
Secured Port Groups view 18
security groups
about 72
add 75
assign resources 76
serial number of vShield Manager 24
services
DNS 22
NTP 23
proxy 23
set clock 101
setup 102
show alerts 109
show arp 109
show clock 109
show configuration 110
show debug 110
show ethernet 111
show filesystem 111
show gateway rules 111
show hardware 112
show hostname 112
show interface 112
show ip addr 113
show ip route 113, 114
show kernel message 114
show kernel message last 115
show log 115
show log alerts 115
show log events 116
show log last 116
show manager log 117
show manager log last 117
show ntp 117
show process 118
Show Report 66
show route 118
show running-config 118
show service 119
show service statistics 119
show services 120
show session-manager counters 120
show session-manager sessions 121
show slots 121

show stacktrace 121
show startup-config 122
show syslog 122
show system events 122
show system load 123
show system memory 123
show system network_connections 123
show system storage 123
show system uptime 124
show tech support 127
show version 124
show vmwall log 124
show vmwall rules 125
shutdown 94
SpoofGuard 77
ssh 127
SSL certificate 24
start or stop vShield Edge services 56
status
of update 37
of vShield Manager 24
vShield App 62
vShield Edge 49
vShield Endpoint 81
SVM alarms for vShield Endpoint 82
csync with vCenter 21
csyncing a vShield App 62
csyntax for CLI commands 90
csyslog
CLI 103
cvShield Edge 50
csyslog format 42
Csyslog Server 61
CSystem Events 41
CSystem Status 62
CForce Sync 62
CRestart 63
traffic stats 63
csystem time 23

T
tactical support log 23
telnet 127
terminal length 130
terminal no length 130
time 23
ttraceroute 128
ttraffic analysis date range 66
ttraffic stats for a vShield App 63

U
uninstall
Port Group Isolation 46
vShield Administration Guide

vShield App 45
vShield Edge 46
vShield Endpoint module 47
vShield Zones 45
unregister a vShield Endpoint SVM 47
Update History 38
Update Status 37
Update User 34
Updates
installing 37
Update History 38
Update Status 37
vShield Edge 56
upgrading a vShield Edge 56
user 129
user interface, logging in 17
Users
adding 34
admin account 34
assigning a role and rights 34
changing a password 34
deleting 35
editing 34
roles and rights 33
V
validate sessions 128
views
Hosts & Clusters 18
Networks 18
Secured Port Groups 18
VM alarms for vShield Endpoint 83
VPN 53
vShield
vShield App 14
vShield Edge 14
vShield Endpoint 15
vShield Manager 13
vShield App
about 14
CLI configuration 62
forcing sync 62
notification based on events 42
restarting 63
sending events to syslog server 61
System Status 62
traffic stats 63
uninstall 45
vShield Edge
about 14
add firewall rule 50
add NAT rules 51
DHCP 52
vShield Zones
about 13
uninstall 45
Zones Firewall 27
vShield Manager
about 13
accessing online help 18
Backups 24
date and time 23
DNS 22
inventory panel 18
logging in 17
notification based on events 42
NTP 23
on-demand backups 39
proxy service 23
restoring a backup 40
scheduling a backup 40
serial number 24
SSL Certificate 24
status 24
Support 23
sync with vCenter Server 21
system events 41
user interface panels 18
vSphere Plug-in 22
vSphere Plug-in 22
W
web-manager 129
write 103
write erase 104
write memory 104

Z

Zones Firewall 27
  adding L2/L3 rules 30
  adding L4 rules 29
  deleting rules 32
  hierarchy of rules 28
  planning rule enforcement 28
  validate sessions 31