Contents

About This Book 9

1 Introduction to the vShield CLI 11
   CLI Command Modes 11
   Logging In and Out of the CLI 12
   CLI Syntax 12
   Moving Around in the CLI 12
   Getting Help within the CLI 13

2 Securing CLI User Accounts 15
   CLI User Account Management 15
   Hardening the CLI of a vShield Virtual Appliance 15
   Add a CLI User Account 16
   Delete the admin User Account from the CLI 16
   Change the CLI Privileged Mode Password 17

3 vShield CLI Commands 19
   Administrative Commands 19
      list 19
      reboot 20
      shutdown 20
   CLI Mode Commands 20
      configure terminal 20
      disable 21
      enable 21
      end 21
      exit 22
      interface 22
      quit 22
   Configuration Commands 23
      clear vmwall rules 23
      cli ssh allow 23
      copy running-config startup-config 24
      database erase 24
      enable password 24
      hostname 25
      ip address 25
      ip name server 26
      ip route 26
      manager key 27
      ntp server 27
      set clock 28
      setup 28
      show configuration 29
      show configuration dhcp 29
      show configuration dns 30
      show configuration firewall 30
      show configuration global 32
show configuration highavailability 32
show configuration interface 33
show configuration ipsec 34
show configuration ipset 35
show configuration loadbalancer 35
show configuration nat 37
show configuration static_routing 37
show configuration syslog 38
show configuration sslvpn-plus 38
slowpath_caps 40
ssh 40
syslog 41
vmwall log suppression 41
write 41
write erase 42
write memory 42

Feature and System Information Commands 42
show arp 42
show arp-filter 43
show fips 43
show firewall 43
show firewall flows 44
show firewall flows topN NUMBER 44
show firewall flows topN NUMBER sort-by pkts 44
show firewall flows topN NUMBER sort-by bytes 44
show firewall rule-id ID 44
show firewall rule-id ID flows 44
show firewall rule-id ID flows topN NUMBER 45
show firewall rule-id ID flows topN NUMBER sort-by pkts 45
show firewall rule-id ID flows topN NUMBER sort-by bytes 45
show flowtable 45
show flowtable rule-id ID 45
show flowtable rule-id ID topN NUMBER 46
show flowtable rule-id ID topN NUMBER sort-by pkts 46
show flowtable rule-id ID topN NUMBER sort-by bytes 46
show flowtable topN NUMBER 46
show flowtable topN NUMBER sort-by pkts 46
show flowtable topN NUMBER sort-by bytes 46
show interface 47
show interface IFNAME 47
show ip route 47
show ip route A.B.C.D/M 47
show nat 47
show service dhcp 48
show service dns 48
show service ipsec 48
show service ipsec cacerts 48
show service ipsec certs 48
show service ipsec crls 48
show service ipsec pubkeys 49
show service ipsec sa 49
show service ipsec sp 49
show service highavailability 49
show service highavailability link 49
show service highavailability connection-sync 50
show service network connections 50
show service sslvpn-plus 50
show service  69
show service helpers  70
show service ipsec  70
show service statistics  71
show services  71
show session-manager counters  71
show session-manager sessions  72
show slots  72
show stacktrace  73
show startup-config  73
show syslog  73
show system cpu  74
show system events  74
show system load  74
show system log size  75
show system memory  75
show system network_connections  75
show system storage  75
show system uptime  76
show version  76
show vmwall log  76
show vmwall rules  77
Diagnostics and Troubleshooting Commands  77
export tech-support scp  77
link-detect  77
ping  78
ping interface addr  78
show tech support  79
ssh  79
telnet  79
traceroute  80
validate sessions  80
vm validation  80
vm validation log  81
User Administration Commands  81
default web-manager password  81
user  81
web-manager  82
Terminal Commands  82
clear vty  82
reset  83
terminal length  83
terminal no length  83
Deprecated Commands  84

Index  85
About This Book

The vShield Command Line Interface Reference describes how to use the VMware® vShield Command Line Interface (CLI) and includes examples and command overviews.

Intended Audience

This guide is intended for anyone who wants to install or use vShield in a VMware vCenter environment. The information in this guide is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This guide 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
- 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.
Introduction to the vShield CLI

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

To use the vShield virtual appliance CLI, you must have console access to a vShield virtual appliance. Each vShield virtual appliance contains a command line interface (CLI). The viewable modes in the vShield CLI can differ based on the assigned role and rights of a user. If you are unable to access an interface mode or issue a particular command, consult your vShield administrator.

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

This chapter includes the following topics:

- “CLI Command Modes” on page 11
- “Logging In and Out of the CLI” on page 12
- “CLI Syntax” on page 12
- “Moving Around in the CLI” on page 12
- “Getting Help within the CLI” on page 13

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 appliance. 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.
Logging In and Out of the CLI

Before you can run CLI commands, you must initiate a console session to a vShield virtual appliance. To open a console session within the vSphere Client, select the vShield virtual appliance 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 XXX command to enable and disable the SSH service on a vShield virtual appliance. See XXX.

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

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 to assist you.

<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 keyword.</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

Each vShield virtual appliance comes with a default user account and password. You should harden the user accounts on each appliance to prevent misuse.

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

This chapter includes the following topics:

- “CLI User Account Management” on page 15
- “Hardening the CLI of a vShield Virtual Appliance” on page 15

**CLI User Account Management**

You must manage CLI user accounts separately on each vShield virtual appliance. By default, you use the admin user account to log in to the CLI of each vShield virtual appliance. 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 appliance.

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 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 appliance 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.

**Hardening the CLI of a vShield Virtual Appliance**

Hardening access to the CLI of a vShield virtual appliance requires addition of a new user account, deletion of the default admin account, and changing of the Privileged mode password.
Add a CLI User Account

You can add a user account with a strong password to secure CLI access to each vShield virtual appliance. 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 and select a vShield virtual appliance from the inventory.
2. Click the Console tab to open a CLI session.
3. Log in by using the admin account.
   
   manager login: admin
   password:
   manager>

4. Switch to Privileged mode.
   
   manager> enable
   password:
   manager#

5. Switch to Configuration mode.
   
   manager# configure terminal

6. Add a user account.
   
   manager(config)# user root password plaintext PASSWORD

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

8. 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 and select a vShield virtual appliance from the inventory.
2. Click the Console tab to open a CLI session.
3. Log in by using a user account other than admin.
4. Switch to Privileged mode.
   
   manager> enable
   password:
   manager#

5. Switch to Configuration mode.
   
   manager# configure terminal

6. Delete the admin user account.
   
   manager(config)# no user admin

7. Save the configuration.
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 and select a vShield virtual appliance from the inventory.
2. Click the Console tab to open a CLI session.
3. Log in to the CLI and switch to Privileged mode.
   
   manager> enable
   password:
   manager#

4. Switch to Configuration mode.
   
   manager# configure terminal

5. Change the Privileged mode password.
   
   manager(config)# enable password PASSWORD

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

7. Run the exit command twice to log out of the CLI.
   
   manager(config)# exit
   manager# exit

8. Log in to the CLI and switch to Privileged mode by using the new password.
   
   manager> enable
   password:
   manager#
The chapter includes the following topics:

- “Administrative Commands” on page 19
- “CLI Mode Commands” on page 20
- “Configuration Commands” on page 23
- “Feature and System Information Commands” on page 42
- “Debug Commands” on page 51
- “Show Commands” on page 57
- “Diagnostics and Troubleshooting Commands” on page 77
- “User Administration Commands” on page 81
- “Terminal Commands” on page 82
- “Deprecated Commands” on page 84

### Administrative Commands

The administrative commands comprise the commands for listing all commands in each CLI mode and for rebooting a or shutting down a vShield virtual appliance.

**List**

Lists all in-mode commands.

**Synopsis**

list

**CLI Mode**

Basic, Privileged, Configuration, Interface Configuration

**Examples**

vShieldMgr> list
enable
exit
list
ping WORD
...

---

**List**

Lists all in-mode commands.

**Synopsis**

list

**CLI Mode**

Basic, Privileged, Configuration, Interface Configuration

**Examples**

vShieldMgr> list
enable
exit
list
ping WORD
...
reboot

Reboots a vShield virtual appliance.

**Synopsis**

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.

**Synopsis**

[no] shutdown

**CLI Mode**

Privileged, Interface Configuration

**Example**

vShield# shutdown

or

vShield(config-if)# shutdown

vShield(config-if)# no shutdown

**Related Commands**

reboot

---

**CLI Mode Commands**

CLI mode commands comprise all of the commands that can be used to change the current mode within the vShield CLI. For more on the different CLI modes, see “CLI Command Modes” on page 11.

configure terminal

Switches to Configuration mode from Privileged mode.

**Synopsis**

configure terminal

**CLI Mode**

Privileged

**Example**

vShield# configure terminal
**disable**

Switches to Basic mode from Privileged mode.

**Synopsis**

disable

**CLI Mode**

Basic

**Example**

vShield# disable
vShield>

**Related Commands**

enable

**enable**

Switches to Privileged mode from Basic mode.

**Synopsis**

enable

**CLI Mode**

Basic

**Example**

vShield> enable
password: enable
vShield#

**Related Commands**

disable

**end**

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

**Synopsis**

disable

**CLI Mode**

Basic, Privileged, Configuration, and Interface Configuration

**Example**

vShield# end
vShield>

**Related Commands**

exit
quit
**exit**

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

**Synopsis**

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.

**Synopsis**

[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.

**Synopsis**

quit
CLI Mode
Basic, Privileged, and Interface Configuration

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

Related Commands
end
exit

Configuration Commands
Configuration commands comprise all of the commands that can be used to configure settings for a vShield virtual appliance.

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 the vShield Administration Guide.

Synopsis
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.

Synopsis
[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 vShield Administration Guide.

Synopsis
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.

Synopsis
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.

Synopsis
enable password PASSWORD

<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>
**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.

**Synopsis**

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>

**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.

**Synopsis**

[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>

**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.

To remove a DNS server, use no before the command.

Synopsis

[no] ip name server A.B.C.D

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

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.

Synopsis

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

Option | Description
--- | ---
A.B.C.D | IP address to use.
M | Subnet mask to use.
W.X.Y.Z | IP address of network gateway.

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.

**Synopsis**

```text
manager key KEY
```  

**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.

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.

**Synopsis**

```text
[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)# 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.

**Synopsis**

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.

**Synopsis**

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>

**show configuration**

Shows the configuration for the vShield Edge.

**Synopsis**

show configuration

**CLI Mode**

Basic

**Related Commands**

show configuration dhcp
show configuration dns
show configuration firewall
show configuration global
show configuration highavailability
show configuration interface
show configuration ipsec
show configuration ipset
show configuration loadbalancer
show configuration nat
show configuration static_routing
show configuration syslog
show configuration sslvpn-plus

**show configuration dhcp**

Shows vShield Edge IP address pooling and one-to-one static IP address allocation.

**Synopsis**

show configuration dhcp

**CLI Mode**

Basic

**Example**

```
{  
  "dhcp" : {  
    "logging" : {  
      "enable" : false,  
      "logLevel" : "info" 
    },  
    "enable" : false,  
    "bindings" : {} 
  }  
}
```
show configuration dns

Shows external DNS servers.

Synopsis

show configuration dns

CLI Mode

Basic

Example

vShield Edge DNS Config:
{
    "dns" : {
        "logging" : {
            "enable" : false,
            "logLevel" : "info"
        },
        "enable" : false,
        "listenOn" : [
            "192.168.2.1"
        ],
        "cacheSize" : 16,
        "forwarders" : [
            "10.20.20.1",
            "10.20.20.2"
        ]
    }
}

show configuration firewall

Shows vShield Edge firewall configuration.

Synopsis

show configuration firewall

CLI Mode

Basic
Example

```json
vShield Edge Firewall Config:
{
    "firewall" : {
        "rules" : [
            {
                "source" : [ "vse" ],
                "dstIface" : [],
                "destination" : [],
                "matchTranslated" : false,
                "sourcePort" : [],
                "description" : "firewall",
                "service" : [],
                "srcIface" : [],
                "logging" : {
                    "enable" : false,
                    "logLevel" : null
                },
                "action" : "accept",
                "id" : 131074
            },
            {
                "source" : [],
                "dstIface" : [],
                "destination" : [ "ipset-32" ],
                "matchTranslated" : false,
                "sourcePort" : [],
                "description" : "lb-in",
                "service" : [ "application-20" ],
                "srcIface" : [],
                "logging" : {
                    "enable" : false,
                    "logLevel" : null
                },
                "action" : "accept",
                "id" : 133125
            },
            {
                "source" : [],
                "dstIface" : [],
                "destination" : [],
                "matchTranslated" : false,
                "service" : [],
                "srcIface" : []
            }
        ]
    }
}
```
show configuration global

Shows configuration for all vShield Edge services.

Synopsis

show configuration global

CLI Mode

Basic

Example

vShield Edge Global Config:
{
  "global" : {
    "enableTcpLoose" : false,
    "hostname" : "vse-930ad822-6fd8-40e6-8544-bec435e032ff-0",
    "fips" : {
      "enable" : false
    },
    "size" : "compact",
    "configurator" : {
      "logging" : {
        "enable" : true,
        "logLevel" : "debug"
      }
    },
    "enableAesni" : true,
    "tenantId" : "3e93fa3b-22f3-4634-a794-f547cd472434",
    "haIndex" : "0"
  }
}

show configuration highavailability

Shows high availability configuration for the vShield Edge.

Synopsis

show configuration highavailability
**CLI Mode**

**Basic**

**Example**

```json
vShield Edge High Availability Config:
{
    "highAvailability": {
        "enable": false,
        "heartbeatInterval": 0,
        "logging": null,
        "security": {
            "enable": true,
            "authenticationSignature": {
               "type": "sha1",
               "key": "a3e1a9af0166235f860323170119cf0efe043e2"
            },
            "encryptionAlgorithm": null
        },
        "interface": null,
        "heartbeatDeadTime": 0,
        "nodes": [],
        "heartbeatWarnTime": 0,
        "heartbeatInitDead": 0
    }
}
```

**show configuration interface**

Shows interfaces configured for the vShield Edge.

**Synopsis**

`show configuration interface`

**CLI Mode**

**Basic**
Example

vShield Edge Interface Config:
{
  "interfaceConfig" : {
    "vNic_9" : {
      "status" : "down",
      "name" : "vnic9",
      "sendRedirects" : true,
      "index" : 9,
      "enableProxyArp" : false,
      "Mac" : "00:50:56:a6:02:3e",
      "Mtu" : 1500,
      "subnets" : []
    },
    "vNic_0" : {
      "status" : "up",
      "name" : "vnic0",
      "sendRedirects" : true,
      "index" : 0,
      "enableProxyArp" : false,
      "Mac" : "00:50:56:a6:6b:9c",
      "Mtu" : 1500,
      "subnets" : [
        {
          "primary" : "10.115.198.241",
          "address" : [
            "10.115.198.241",
            "10.115.198.242"
          ],
          "subnet" : "10.115.198.0/23"
        }
      ]
    },
    "vNic_7" : {
      "status" : "down",
      "name" : "vnic7",
      "sendRedirects" : true,
      "index" : 7,
      "enableProxyArp" : false,
      "Mac" : "00:50:56:a6:f0:cd",
      "Mtu" : 1500,
      "subnets" : []
    }
  }
}

show configuration ipsec

Shows certificate configuration for IPSec VPN.

Synopsis

show configuration ipsec

CLI Mode

Basic
show configuration ipset

Shows IP address groups defined at the vShield Edge scope.

Synopsis

show configuration ipset

CLI Mode

Basic

Example

```json
vShield Edge IPsec VPN Config:
{
    "ipsec" : {
      "logging" : {
        "enable" : false,
        "logLevel" : "info"
      },
      "enable" : false,
      "sites" : [],
      "global" : {
        "serviceCertificate" : null,
        "crlCertificates" : [],
        "pskForDynamicIp" : null,
        "id" : null,
        "caCertificates" : []
      }
    }
}
```

show configuration loadbalancer

Shows external, or public, IP address mapped to internal servers for load balancing.

Synopsis

show configuration loadbalancer

CLI Mode

Basic
Example

vShield Edge Loadbalancer Config:
{
  "loadBalancer": {
    "enable": true,
    "listeners": [
      {
        "listenerIpAddresses": ["10.115.198.243:80"],
        "algorithm": "round-robin",
        "logging": {
          "enable": false,
          "logLevel": "info"
        },
        "backendServers": [
          {
            "ipAddress": "192.168.2.2",
            "weight": 1,
            "port": 80,
            "healthcheck": {
              "rise": null,
              "fall": null,
              "timeout": null,
              "mode": null,
              "port": 80,
              "interval": null,
              "uri": null
            }
          },
          {
            "ipAddress": "192.168.2.3",
            "weight": 1,
            "port": 80,
            "healthcheck": {
              "rise": null,
              "fall": null,
              "timeout": null,
              "mode": null,
              "port": 80,
              "interval": null,
              "uri": null
            }
          }
        ]
      }
    ]
  }
}
show configuration nat

Shows NAT rules defined for the vShield Edge.

**Synopsis**

```
show configuration nat
```

**CLI Mode**

Basic

**Example**

```
vShield Edge NAT Config:
{
  "dnat": [
    {
      "protocol": "G",
      "internalIp": "10.115.198.243",
      "externalPort": "80",
      "comments": "loadBalancer",
      "ruleId": 200709,
      "icmpType": null,
      "logging": {
        "enable": false,
        "logLevel": null
      },
      "internalPort": "80",
      "externalIp": "10.115.198.243",
      "interface": "vmNic_0"
    }
  ],
  "snat": []
}
```

show configuration static_routing

Shows the static routes defined for the vShield Edge data packets.

**Synopsis**

```
show configuration static_routing
```
**CLI Mode**

Basic

**show configuration syslog**

Shows remote syslog servers defined for the vShield Edge.

**Synopsis**

show configuration syslog

**CLI Mode**

Basic

**Example**

```
vShield Edge Syslog Config:
{
    "syslog" : { 
        "protocol" : null,
        "destinationHost" : []
    }
}
```

**show configuration sslvpn-plus**

Shows the SSL VPN configuration.

**Synopsis**

show configuration sslvpn-plus

**CLI Mode**

Basic
Example

```json
vShield Edge SSL VPN-Plus Config:
{
  "sslvpn": {
    "enable": false,
    "webResources": [],
    "users": [],
    "serverSettings": null,
    "activeSessions": null,
    "advancedConfiguration": {
      "enableSso": null,
      "enablePublicUrlAccess": false,
      "forceVirtualKeyboard": false,
      "randomizeVirtualKeys": false,
      "clientNotification": "",
      "preventMultipleLogon": false,
      "sessionIdleTimeout": 10,
      "domainName": null,
      "enableCompression": false,
      "forcedTimeout": 0
    },
    "clientInstallPackages": [],
    "layoutConfiguration": {
      "rowColor": "F5F5F5",
      "logoBackgroundColor": "FFFFFF",
      "portalLogoName": "portal_logo_default.jpg",
      "bodyColor": "FFFFFF",
      "fileVersion": 0,
      "MenuBarColor": "999999",
      "titleColor": "996600",
      "connectedIconHash": null,
      "phatBannerHash": null,
      "topFrameColor": "000000",
      "errorIconHash": null,
      "portalTitle": "VMware",
      "rowAlternativeColor": "FFFFFF",
      "desktopIconHash": null,
      "companyName": "VMware",
      "portalLogoHash": "99d8a112297310491f7fc1aade527d54",
      "disConnectedIconHash": null
    },
    "logging": {
      "enable": false,
      "logLevel": "info"
    },
    "clientConfiguration": {
      "gatewayIp": null,
      "fullTunnel": false,
```
slowpath_caps

Starts, stops, or shows slowpath offload capabilities.

**Synopsis**

slowpath_caps (show | start | stop)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Shows slowpath offload capabilities.</td>
</tr>
<tr>
<td>start</td>
<td>Starts slowpath offload.</td>
</tr>
<tr>
<td>stop</td>
<td>Stops slowpath offload.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Basic

**ssh**

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

**Synopsis**

ssh (start | stop)

**CLI Mode**

Basic

**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.

To disable syslog export, use no before the command.

Synopsis

[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

vmwall log suppression

Enables or disables the suppression of VMWall logs.

Synopsis

vmwall log suppression (disable | enable)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the suppression of VMWall logs.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the suppression of VMWall logs.</td>
</tr>
</tbody>
</table>

CLI Mode

Basic

Example

vShield# vmwall log suppression disable

write

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

Synopsis

write
CLI Mode
Privileged

Example
manager# write

Related Commands
write memory

write erase
Resets the CLI configuration to factory default settings.

Synopsis
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.

Synopsis
write memory

CLI Mode
Privileged, Configuration, and Interface Configuration

Example
manager# write memory

Related Commands
write

Feature and System Information Commands
The feature commands help you monitor vShield Edge states and statistics.

show arp
Shows the Address Resolution Protocol (ARP) settings for the vShield Edge.

Synopsis
show arp

CLI Mode
Basic
Example

```
vShield Edge ARP Cache:
fe80::214:f07:c0f8:27f0 dev vNic_0 lladdr 00:14:f6:f8:27:f0 route
10.115.198.243 dev vNic_0 lladdr 00:50:56:2b:00:00 REACHABLE
169.254.0.2 dev vNic_1 lladdr 00:50:56:a6:41:43 PERMANENT
10.115.199.253 dev vNic_0 lladdr 00:14:f6:f8:27:f0 STALE
10.115.199.245 dev vNic_0 FAILED
```

show arp-filter
Displays the ARP packet filter rules that specify what to do with a packet that matches.

Synopsis
```
show arp-filter
```

CLI Mode
Basic

Example

```
vShield Edge ARP Filter Table:
Chain IN (policy ACCEPT 1116K packets, 31M bytes)
   pkts bytes target in out source-ip dest source-hw destination-hw hlen op hrd

Chain OUT (policy ACCEPT 14798 packets, 414K bytes)
   pkts bytes target in out source-ip dest source-hw destination-hw hlen op hrd

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
   pkts bytes target in out source-ip dest source-hw destination-hw hlen op hrd
```

show fips
Indicates whether Federal Information Processing Standard (FIPS) is disabled for the specified vShield Edge.

Synopsis
```
show fips
```

CLI Mode
Basic

show firewall
Displays firewall packet counters along with firewall rules that specify what to do with a packet that matches.

Synopsis
```
show firewall
```

CLI Mode
Basic
show firewall flows
Displays the firewall packet counters along with packet flows.

Synopsis
show firewall flows

CLI Mode
Basic

show firewall flows topN NUMBER
Displays firewall packet counters along with top N number of packet flows.

Synopsis
show firewall flows top 10

CLI Mode
Basic

show firewall flows topN NUMBER sort-by pkts
Displays firewall packet counters along with top N number of packet flows sorted by packet numbers.

Synopsis
show firewall flows top 10 sort-by-pkts

CLI Mode
Basic

show firewall flows topN NUMBER sort-by bytes
Displays firewall packet counters along with top N number of packet flows sorted by byte numbers.

Synopsis
show firewall flows top 10 sort-by-bytes

CLI Mode
Basic

show firewall rule-id ID
Displays firewall packet counters filtered by rule-id.

Synopsis
show firewall rule-id 25

CLI Mode
Basic

show firewall rule-id ID flows
Displays firewall packet counters filtered by rule-id.
**Synopsis**

show firewall rule-id 25 flows

**CLI Mode**

Basic

**show firewall rule-id ID flows topN NUMBER**

Displays firewall packet counters filtered by rule-id along with top N number of packet flows.

**Synopsis**

show firewall rule-id 25 flows top 10

**CLI Mode**

Basic

**show firewall rule-id ID flows topN NUMBER sort-by pkts**

Displays firewall packet counters filtered by rule-id along with top N number of packet flows sorted by packet numbers.

**Synopsis**

show firewall rule-id 25 flows top 10 sort-by-pkts

**CLI Mode**

Basic

**show firewall rule-id ID flows topN NUMBER sort-by bytes**

Displays firewall packet counters filtered by rule-id along with top N number of packet flows sorted by byte numbers.

**Synopsis**

show firewall rule-id 25 flows top 10 sort-by-bytes

**CLI Mode**

Basic

**show flowtable**

Displays packet flows in a table.

**Synopsis**

show flowtable

**CLI Mode**

Basic

**show flowtable rule-id ID**

Displays packet flows matched by rule-id.

**Synopsis**

show flowtable rule-id 25
CLI Mode
Basic

**show flowtable rule-id ID topN NUMBER**
Displays the top $N$ number of packet flows matched by rule-id.

**Synopsis**
```
show flowtable rule-id 25
```

**show flowtable rule-id ID topN NUMBER sort-by pkts**
Displays the top $N$ number of packet flows matched by rule-id sorted by packet numbers.

**Synopsis**
```
show flowtable rule-id 25
```

**show flowtable rule-id ID topN NUMBER sort-by bytes**
Displays top $N$ number of packet flows matched by rule-id sorted by byte numbers.

**Synopsis**
```
show flowtable rule-id 25
```

**show flowtable topN NUMBER**
Displays top $N$ number of packet flows.

**Synopsis**
```
show flowtable top 10
```

**show flowtable topN NUMBER sort-by pkts**
Displays top $N$ number of packet flows sorted by packet numbers.

**Synopsis**
```
show flowtable top 10 sort-by pkts
```

**show flowtable topN NUMBER sort-by bytes**
Displays top $N$ number of packet flows sorted by byte numbers.
Chapter 3  vShield CLI Commands

Synopsis
show flowtable top 10 sort-by bytes

CLI Mode
Basic

show interface
Displays interface information like IP addresses.

Synopsis
show interface

CLI Mode
Basic

show interface IFNAME
Displays interface information for the specified interface.

Synopsis
show interface TEST

CLI Mode
Basic

show ip route
Displays the IP routing table used to calculate the destination of the packet it is responsible for forwarding.

Synopsis
show ip route

CLI Mode
Basic

show ip route A.B.C.D/M
Displays a route entry matched by the specified prefix.

Synopsis
show ip route A.B.C.D

CLI Mode
Privileged, Configuration, and Interface Configuration

show nat
Displays NAT packet counters along with the NAT rules that specify how to translate network addresses for a packet that matches.

Synopsis
show nat
**show service dhcp**

Displays whether the DHCP service is running.

**Synopsis**

`show service dhcp`

**CLI Mode**

Basic

**show service dns**

Displays whether the DNS service is running.

**Synopsis**

`show service dhcp`

**CLI Mode**

Basic

**show service ipsec**

Displays whether the VPN IPSEC service is running.

**Synopsis**

`show service ipsec`

**CLI Mode**

Basic

**show service ipsec cacerts**

Displays IPSEC CA certificates configured for the vShield Edge.

**Synopsis**

`show service ipsec cacerts`

**CLI Mode**

Privileged, Configuration, and Interface Configuration

**show service ipsec certs**

Displays IPSEC certificates configured for the vShield Edge.

**Synopsis**

`show service ipsec certs`

**CLI Mode**

Basic

**show service ipsec crls**

Displays Certificate Revocation List (CRL) configured for the vShield Edge.
show service ipsec pubkeys
Displays all installed public keys that are either received from peers or loaded locally.

show service ipsec sa
Displays the security association database, which contains a set of security information that describes a particular kind of secure connection between one device and another.

show service ipsec sp
Displays the security policy database, which contains a set of rules that are programmed into the IPSec implementation that tells it how to process different packets received by the device.

show service highavailability
Displays high availability (HA) service information such as HA status and Healthcheck status, etc.

show service highavailability link
Displays HA link information such as IP addresses for peer links and local links.
show service highavailability connection-sync
Displays HA connection sync-up status information. For example, statistics about current active connections of both local and peer device.

Synopsis
show service highavailability connection-sync

show service network connections
Displays service network connection information. For example, TCP and UDP service information.

Synopsis
show service network connections

show service sslvpn-plus
Displays SSL VPN-Plus service information.

Synopsis
show service sslvpn-plus

show service sslvpn-plus stats
Displays SSL VPN-Plus statistic information.

Synopsis
show service sslvpn-plus stats

show service sslvpn-plus sessions
Displays SSL VPN-Plus active sessions.

Synopsis
show service sslvpn-plus sessions
show service sslvpn-plus tunnels
Displays SSL VPN-Plus tunnel information.

Synopsis
show service sslvpn-plus tunnels

CLI Mode
Basic

show system network-stats
Displays network statistics. For example, statistics for IP, ICMP, TCP and UDP, etc.

Synopsis
show system network-stats

CLI Mode
Basic

Debug Commands
Debug commands allow you to troubleshoot issues by resetting system counters, monitoring network traffic, sending packets to other ends, or checking network availability.

clear firewall counters
Resets firewall counters to zeros.

Synopsis
clear firewall counters

CLI Mode
Basic

clear nat counters
Resets NAT counters to zeros.

Synopsis
clear nat counters

CLI Mode
Privileged, Configuration, and Interface Configuration

clear arp WORD
Deletes an ARP entry from the ARP table, which is associated with the specified IP address.

Synopsis
clear arp WORD

CLI Mode
Basic
clear service dhcp lease

Removes DHCP lease information from the DHCP service.

**Synopsis**
clear service dhcp lease

**CLI Mode**
Basic

clear service ipsec sa WORD

Deletes the SA (Security Association) associated with the specified peer name.

**Synopsis**
clear service ipsec sa WORD

**CLI Mode**
Basic

dnslookup server

Makes DNS lookup query to the specified DNS server.

**Synopsis**
dnslookup server

**CLI Mode**
Basic

dnslookup server name_or_address

Makes DNS lookup query for the specified host or IP address.

**Synopsis**
dnslookup server name_or_address

**CLI Mode**
Basic

debug copy

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

**Synopsis**
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 userid@&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>
</tbody>
</table>
### debug crashdump

Activates crash dump support and triggers a reboot. After the reboot, vShield Edge runs with crashkernel support active. When a kernel panic occurs, vShield Edge boots the crash kernel and stores the kernel dump to the file system. Edge then reboots again back into the standard kernel, with crashdump still enabled.

To view the kernel dump file, use `debug show files`.

To copy the kernel dump file, use `debug copy [ftp|scp] ...`

To delete the kernel dump file, use `debug remove [<filename>|all]`.

When crashdump is enabled, the available vShield Edge memory is reduced by 64MB. To disable crashdump support, type `no debug crashdump`.

The `debug crashdump` command is not supported for the 64 bit X-Large vShield Edge.

### Synopsis

ddebug crashdump

### CLI Mode

Privileged

### Usage Guidelines

vShield Edge CLI

### Related Commands

ddebug show files
ddebug copy
ddebug remove
**debug 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.

**Synopsis**

```plaintext
[no] debug packet capture (segment 0 | interface (mgmt | c0 | d0 | u0 | p0)) [EXPRESSION] [REALMID]
```

<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>c0</td>
</tr>
<tr>
<td>EXPRESSION</td>
<td>A tcpdump-formatted string. You must use an underscore between words in the expression.</td>
</tr>
<tr>
<td>REALMID</td>
<td>The realm ID of the u0 or p0 interface from which to capture packets.</td>
</tr>
</tbody>
</table>

**CLI Mode**

Privileged

**Usage Guidelines**

vShield App CLI

**Example**

```plaintext
vShield# debug packet capture segment 0 host_10.10.11.11_port_8
```

**Related Commands**

debag copy
debag packet display interface

debag packet display interface

**debug packet display interface**

Displays contents of packets on the specified network interface.

**Synopsis**

```plaintext
debag packet display interface
```

**CLI Mode**

Basic

**debug 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.

**Synopsis**

```plaintext
vShield App
[no] debug packet display interface (mgmt | u0 | p0) [EXPRESSION]
```
vShield App or vShield Edge CLI

Example

vShield# debug packet display interface mgmt host_10.10.11.11_and_port_80

Related Commands

debug packet capture  

**debug remove**

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

**Synopsis**

debug 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# debug remove tcpdumps all

**Related Commands**

depug copy  
depug packet capture  
depug show files
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.

Synopsis

[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-FTP-Dynamic-Port-Detection sysmgr high

Related Commands

show services

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.

Synopsis


<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>
<tr>
<td>W.X.Y.Z</td>
<td>Destination IP address of use.</td>
</tr>
<tr>
<td>M</td>
<td>Destination subnet mask to use.</td>
</tr>
<tr>
<td>P</td>
<td>Destination 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**

**Related Commands**
show services

default show files
Shows the tcpdump files that have been saved.

**Synopsis**
default 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**
default copy
default remove

default tech-support
Displays system information for tech-support. It shows all the information contained in tech-support tarball file.

**Synopsis**
show tech-support

**CLI Mode**
Basic

**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.

**Synopsis**
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**

```
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.

**Synopsis**

```
show arp
```

**CLI Mode**

Basic, Privileged

**Example**

```
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).

**Synopsis**

```
show clock
```

**CLI Mode**

Basic, Privileged

**Example**

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

**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.

**Synopsis**

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 IPsec 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.

**Synopsis**

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 debug log

Shows the system debug log.

**Synopsis**

show debug log [follow | reverse]
### CLI Mode

**Basic**

**Example**

vShield# show debug log follow
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[21466]: 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
...

**show dvf-support**

Shows the DVFilter system information.

**Synopsis**

show dvf-support

**CLI Mode**

Basic

**show ethernet**

Shows Ethernet information for virtual machine interfaces.

**Synopsis**

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.
**Synopsis**

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.

**Synopsis**

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.

**Synopsis**

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
 +00.0  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)
show hostname

Shows the current hostname for a vShield Edge.

Synopsis

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.

Synopsis

show interface [c0 | d0 | mgmt | p0 | u0]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c0</td>
<td>vShield App C0 interface</td>
</tr>
<tr>
<td>d0</td>
<td>vShield App D0 interface</td>
</tr>
<tr>
<td>mgmt</td>
<td>Management interface</td>
</tr>
<tr>
<td>p0</td>
<td>vShield App P0 interface</td>
</tr>
<tr>
<td>u0</td>
<td>vShield App port U0 interface</td>
</tr>
</tbody>
</table>

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, frame 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.
**Synopsis**

show ip addr

**CLI Mode**

Basic, Privileged

**Example**

vShield# show ip addr

**show ip route**

Shows the IP routing table.

**Synopsis**

show ip route [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**

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.

**Synopsis**

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.

Synopsis

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.

Synopsis

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.

Synopsis

show log [last | follow | reverse]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>last $N$</td>
<td>Show the last $N$ lines of the log.</td>
</tr>
<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[21466]: 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.

**Synopsis**

`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.

**Synopsis**

`show log events`

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield App CLI

**Example**

vShield# show log events
Related Commands

show log

show log follow

Displays the log as it gets log contents.

Synopsis

show log follow

CLI Mode

Basic

Usage Guidelines

vShield Edge

show log last

Shows last $n$ lines of the log.

Synopsis

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 log reverse

Displays the log in reverse chronological order.

Synopsis

show log reverse

CLI Mode

Basic

Usage Guidelines

vShield Edge
show manager log

Shows the system log of the vShield Manager.

**Synopsis**

```
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>
<tr>
<td>size</td>
<td>Display manager log size.</td>
</tr>
<tr>
<td>last n</td>
<td>Display the last n number of events in the vShield Manager log.</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 Debug 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.

**Synopsis**

```
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.

**Synopsis**

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.

**Synopsis**

show process (list | monitor)

**Option** | **Description**
---|---
list | List all currently running processes on the vShield Edge.
monitor | Continuously monitor the list of processes.

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield Edge CLI

**Example**

vShieldEdge# show process list

---

show realms

Shows the current realms on a vShield Edge.

**Synopsis**

show realms

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield App CLI
**Example**

vShieldEdge# show realms

**show route**

Shows the current routes configured on a vShield Edge.

**Synopsis**

show route

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield Edge CLI

**Example**

vShieldEdge# show route

**show running-config**

Shows the current running configuration.

**Synopsis**

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.

**Synopsis**

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

Usage Guidelines
vShield Edge CLI

Example
vShieldEdge# show service dhcp

**show service helpers**

Shows all service helpers for a specific realm.

**Synopsis**

show service helpers REALMID

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REALMID</td>
<td>The realm ID.</td>
</tr>
</tbody>
</table>

CLI Mode
Basic

Usage Guidelines
vShield App CLI

Example
vShieldEdge# show service helpers 1024

**show service ipsec**

Shows the VPN service details.

**Synopsis**

show service ipsec (cacerts | certs | ctrls | pubkeys | sa | sp | status)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacerts</td>
<td>Show the CA certificates.</td>
</tr>
<tr>
<td>certs</td>
<td>Show the Edge certificates</td>
</tr>
<tr>
<td>ctrls</td>
<td>Show the CRLs revoke certificates.</td>
</tr>
<tr>
<td>pubkeys</td>
<td>Show the public keys.</td>
</tr>
<tr>
<td>sa</td>
<td>Show the Security Association Database (SAD) entry.</td>
</tr>
<tr>
<td>sp</td>
<td>Show the Security Policy Database (SPD) entry.</td>
</tr>
<tr>
<td>status</td>
<td>Show the status of the ipsec server.</td>
</tr>
</tbody>
</table>

CLI Mode
Basic

Usage Guidelines
vShield Edge CLI
Example

vShieldEdge# show service ipsec status

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.

Synopsis

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.

Synopsis

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

show 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.
**Synopsis**

show 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_STATS_SockCreated 61
SA_TCP_STATS_NewSynReceived 61
SA_TCP_STATS_RetransSynReceived 0

**Related Commands**

show session-manager sessions

**show session-manager sessions**

Shows the current sessions in process on a vShield App.

**Synopsis**

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.

**Synopsis**

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.

Synopsis

show stacktrace

CLI Mode

Basic, Privileged

Example

vShield# show stacktrace

show startup-config

Shows the startup configuration.

Synopsis

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.

Synopsis

show syslog

CLI Mode

Basic, Privileged

Example

vShield# show syslog
*.* ~/var/log/messages
*. emerg /dev/tty1

Related Commands

syslog
show system cpu

Shows the system cpu details.

**Synopsis**

show system cpu

**CLI Mode**

Basic

**Example**

vShield# show system cpu

**Related Commands**

show system memory
show system uptime

show system events

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

**Synopsis**

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.

**Synopsis**

show system memory

**CLI Mode**

Basic, Privileged

**Usage Guidelines**

vShield Edge CLI

**Example**

vShield# show system mem
MemTotal: 2072204 kB
MemFree: 1667248 kB
show system log size

Shows the total size of the system log files.

Synopsis

show system log size

CLI Mode

Basic

Example

vShield# show system log size
1M

show system memory

Shows the summary of memory utilization.

Synopsis

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.

Synopsis

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.

Synopsis

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.

**Synopsis**
`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.

**Synopsis**
`show version`

**CLI Mode**
Basic, Privileged

**Example**
vShield# show version

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

**Synopsis**
`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.

Synopsis
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.

Synopsis
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.
**Synopsis**

[no] link-detect

**CLI Mode**

Interface Configuration

**Example**

vShield(config-if)# link-detect

or

evShield(config-if)# no link-detect

---

**ping**

Pings a destination by its hostname or IP address.

**Synopsis**

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

**Option** | **Description**
--- | ---
HOSTNAME | A.B.C.D | The hostname or IP address of the target system.

**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.

**Synopsis**

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

**Option** | **Description**
--- | ---
SOURCE_HOSTNAME | A.B.C.D | The hostname or internal IP address of a virtual machine protected by a vShield Edge.

DEST_HOSTNAME | A.B.C.D | The hostname or IP address of the destination.

**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.

Synopsis
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.

Synopsis
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.

Synopsis
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.

**Synopsis**

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.

**Synopsis**

validate sessions

**CLI Mode**

Privileged

**Usage Guidelines**

vShield App CLI

**Example**

vShieldApp# validate sessions

**vm validation**

Shows the status of, starts, or stops the virtual machine validation functionality.

**Synopsis**

vm validation (disable | enable | status)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the virtual machine validation functionality.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the virtual machine validation functionality.</td>
</tr>
<tr>
<td>status</td>
<td>Shows the status of the virtual machine validation functionality.</td>
</tr>
</tbody>
</table>
**CLI Mode**
Privileged

**Usage Guidelines**
vShield App CLI

**Example**
```
vShieldApp# vm validation enable
```

### vm validation log

Shows the dropped or allowed packets due to virtual machine validation functionality.

**Synopsis**
```
vm validation log (accepted | dropped)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accepted</td>
<td>Shows the allowed packets due to virtual machine validation functionality.</td>
</tr>
<tr>
<td>dropped</td>
<td>Shows the dropped packets due to virtual machine validation functionality.</td>
</tr>
</tbody>
</table>

**CLI Mode**
Privileged

**Usage Guidelines**
vShield App CLI

**Example**
```
vShieldApp# vm validation log accepted
```

### User Administration Commands

**default web-manager password**

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

**Synopsis**
```
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.

**Synopsis**

```
[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 <code>show running-config</code> 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.

**Synopsis**

```
[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.
**Synopsis**
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.

**Synopsis**
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.

**Synopsis**
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.

**Synopsis**
terminal no length
CLI Mode
Privileged

Example
manager# terminal no length

Related Commands
reset
terminal length

Deprecated Commands
The following table lists deprecated commands.

Table 3-1. 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>
Index

B
- basic mode of CLI 11

C
- clear vmwall rules 23
- clear vty 82

CLI
- configuration mode 11
- help 13
- interface mode 11
- logging in 12
- modes 11, 12
- privileged mode 11
- syntax 12
- command syntax 12
- configuration mode of CLI 11
- configure terminal 20
- copy running-config startup-config 24

D
- database erase 24
- debug copy 52
- debug crashdump 53
- debug packet capture 54
- debug packet display interface 54
- debug remove 55
- debug service 56
- debug service flow src 56
- debug show files 57
- default web-manager password 81
- disable 21

E
- enable 21
- enable password 24
- end 21
- exit 22
- export tech-support scp 77

H
- help
  - CLI 13
- hostname 25

I
- interface 22
- interface mode of CLI 11

ip address 25
- ip name server 26
- ip route 26

L
- link-detect 77
- login
  - CLI 12

M
- manager key 27

N
- ntp server 27

P
- ping 78
- ping interface addr 78
- privileged mode of CLI 11

Q
- quit 22

R
- reboot 20
- reset 83

S
- set clock 28
- setup 28
- show alerts 57
- show arp 58
- show clock 58
- show configuration 59
- show debug 59
- show debug log 59
- show dvf-support 60
- show ethernet 60
- show filesystem 60
- show gateway rules 61
- show hardware 61
- show hostname 62
- show interface 62
- show ip addr 62
- show ip route 63
- show kernel message 64
- show kernel message last 64
show log 64
show log alerts 65
show log events 65
show log last 66
show manager log 67
show manager log last 67
show ntp 68
show process 68
show realms 68
show route 69
show running-config 69
show service 69
show service helpers 70
show service ipsec 70
show service statistics 71
show services 71
show session-manager counters 71
show session-manager sessions 72
show slots 72
show stacktrace 73
show startup-config 73
show syslog 73
show system cpu 74
show system events 74
show system load 74, 75
show system memory 75
show system network_connections 75
show system storage 75
show system uptime 76
show tech support 79
show version 76
show vmwall log 76
show vmwall rules 77
shutdown 20
slowpath_caps 40
ssh 79
syntax for CLI commands 12

telnet 79
terminal length 83
terminal no length 83
traceroute 80

T

telnet 79
terminal length 83
terminal no length 83
traceroute 80

U

user 81

V

validate sessions 80
vm validation 80
vm validation log 81

vmwall log suppression 41

W

web-manager 82
write 41
write erase 42
write memory 42