DDoS Secure

CLI User Guide

Release
5.14.1-0

Published: 2014-05-14

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

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

DDoS Secure CLI User Manual

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

Part 2

List of Figures

Part 2

List of Tables

Part 1 CLI Overview

Part 2

About the Documentation

Documentation and Release Notes

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

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

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

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

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

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

Documentation Feedback

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

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

CLI Overview

CHAPTER 1

Command-Line Overview

This chapter includes gives an overview of the DDoS Secure CLI and describes the available show commands.

Introducing the DDoS Secure CLI

The command-line interface (CLI) provides a simple command syntax for the purpose of making configuration changes to a DDoS Secure appliance. The CLI can be accessed in one of three ways:

- ANSI terminal software through a serial line connection to the appliance serial port.
- SSH connection to the appliance management interface.
- System console with the use of a keyboard and monitor.

Related Documentation

- Connecting to a DDoS Appliance Using a System Console Connection on page 5
- Starting a CLI Session on page 5
- Connecting to a DDoS Appliance Using an SSH Connection on page 4

Connecting to a DDoS Appliance Using a Serial Port Connection

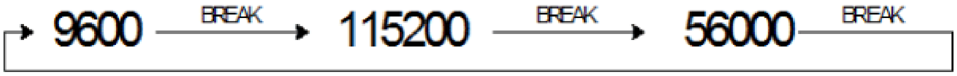
The serial port is located on the back of the DDoS Secure appliance and uses industry-standard pinouts.

To communicate with the appliance (the serial port on the device that the appliance is connected to), set one of the following:

- 9600 baud, 1 stop bit, no parity, and hardware flow control.
- 57600 baud, 1 stop bit, no parity, and hardware flow control.
- 115200 baud, 1 stop bit, no parity, and hardware flow control.

The appliance displays the hardware initialization and booting diagnostic messages at 9600 baud. This is the recommended speed to use for troubleshooting.

To switch to a faster speed for normal system management, it is necessary to send a BREAK to switch to the next available speed, followed by two or three RETURN or LINE-FEED characters. Each time a BREAK is sent, the speed cycles between the supported speeds in the following order:



Related Documentation

- DDoS Secure Appliance Panel Information on page 279
- Connecting to a DDoS Appliance Using a System Console Connection on page 5
- Starting a CLI Session on page 5
- Connecting to a DDoS Appliance Using an SSH Connection on page 4

Connecting to a DDoS Appliance Using an SSH Connection

To use the CLI through the Internet SSH protocol:

1. The DDoS Secure appliance management interface must first be configured with an appropriate IP address, network mask, default gateway, and the interface speed.
2. SSH access from the client IP address must be enabled.

For the detailed procedure, see the *DDoS Secure GUI User Guide*. Once enabled, the configuration can be modified through the CLI.

Related Documentation

- Connecting to a DDoS Appliance Using a Serial Port Connection on page 4
- Connecting to a DDoS Appliance Using a System Console Connection on page 5
- Starting a CLI Session on page 5

Connecting to a DDoS Appliance Using a System Console Connection

The system console operates like a PC that supports a USB or PS2 style keyboard, and a SVGA monitor.

Related Documentation

- Connecting to a DDoS Appliance Using an SSH Connection on page 4
- Starting a CLI Session on page 5
- Connecting to a DDoS Appliance Using a Serial Port Connection on page 4

Starting a CLI Session

To start a CLI session, you must authenticate to the CLI subsystem using one of the authentication methods. The initial default user is **user**, and the default password is **password**.

NOTE: **We recommend that you change the default authentication credentials as soon as possible.**

Example login using the console or a serial interface:

```
DDoS Secure appliance version 5.14.1.0
```

ws_192_168_0_196 login: user
Password: password
JS>sh version

```
DDoS Secure Code Version:      5.14.1-0
DDoS Secure Code Base:         CENTOS_6_3
DDoS Secure Build Date:        201305201820GMT
CD Base Image:                 5.14.1-0
Actual Memory Size:            31.3G
Actual Number of CPUs:         16
Serial No:                     A1RYMW1
Hardware ID:                   90:B1:1C:2A:A3:28
Platform:                      J-DDOS-SEC-AP2
Last Restart:                  Tue May 21 16:54:09 2013
Licensed Throughput:           10G
Memory To Use:                 31G
CPUs To Use:                   16
Protected IPs Supported:       64K
Tracked IPs Supported:         32M
Portals Supported:             256
Filters Supported:             4K
MAC Entries Supported:         16K
TCP Entries Supported:         4M
UDP Entries Supported:         512K
ICMP Entries Supported:        64K
Other IP Entries Supported:    64K
Fragment Entries Supported:    32K
FTP Entries Supported:         8K
SSL Decoders Supported:        512K
SSL Sessions Supported:        512K
SSL Handshake Buffers:         1K
SSL Block Buffers:             2K
SSL Key Exchanges Supported:   512K
```

JS>

Example login using SSH from the Unix command line:

```
Prompt>ssh –l user 192.168.0.196
user@192.168.0.196s user’s password:password
JS>sh version

DDoS Secure Code Version:      5.14.1-0
DDoS Secure Code Base:         CENTOS_6_3
DDoS Secure Build Date:        201305201820GMT
CD Base Image:                 5.14.1-0
Actual Memory Size:            31.3G
Actual Number of CPUs:         16
Serial No:                     A1RYMW1
Hardware ID:                   90:B1:1C:2A:A3:28
Platform:                      J-DDOS-SEC-AP2
Last Restart:                  Tue May 21 16:54:09 2013
Licensed Throughput:           10G
Memory To Use:                 31G
CPUs To Use:                   16
Protected IPs Supported:       64K
Tracked IPs Supported:         32M
Portals Supported:             256
Filters Supported:             4K
MAC Entries Supported:         16K
TCP Entries Supported:         4M
UDP Entries Supported:         512K
ICMP Entries Supported:        64K
Other IP Entries Supported:    64K
Fragment Entries Supported:    32K
FTP Entries Supported:         8K
SSL Decoders Supported:        512K
SSL Sessions Supported:        512K
SSL Handshake Buffers:         1K
SSL Block Buffers:             2K
SSL Key Exchanges Supported:   512K
```

JS>

For more information about how users are allocated to different portals (virtual subappliances) and how users can gain access to the CLI to allow configuration of their individual portals, see the *DDoS Secure GUI User Guide*. If the portal is not the master portal (**-General-**), then it is indicated in the prompt as follows:

```
Prompt>  ssh –l user 192.168.0.196
user@192.168.0.196s user’s password:password
JS portal>show config
version e2
configuration portal
remove user all
remove server all
remove fagg all
remove filter all
set operation mode defensive countries all aslist all
set user portaluser password $1$blI73sjE$wA.A7vHC1qvdfROlEHJtM. perms administrator
...
set mail server none dailystats yes alerts no
```

```
JS portal>
```

If the CLI connection is to the Standby member of an Active/Standby pair, then the prompt also includes (Standby):

```
JS(Standby)>
```

or

```
JS(Standby) portal>
```

Related Documentation

- Connecting to a DDoS Appliance Using a Serial Port Connection on page 4
- Connecting to a DDoS Appliance Using an SSH Connection on page 4
- Navigating Through the CLI on page 7
- Connecting to a DDoS Appliance Using a System Console Connection on page 5

Navigating Through the CLI

The CLI environment has shortcuts and built-in help messages to aid in the configuration of the DDoS Secure appliance.

When you enter a command or the name of a parameter, it is not necessary to type the full name. A command can be abbreviated to the smallest sequence of characters that uniquely identifies the command.

- To automatically complete the current command you are typing, press Tab. If the command cannot be completed, press Tab again to display a brief list of available matching commands. Once you have entered a command, press Tab to complete the next parameter. If there is more than one option available, pressing Tab displays the available valid parameters. If this is in the middle of a free-text input parameter value field, terminate the field with a space first.

NOTE: **If the command is a free-text value field, you must complete the field with a space character before you press the Tab key.**

- Press the up and down arrow keys to display the previously entered commands.
- Use the left and right arrow keys to move back and forth along the text line currently displayed; this allows you to edit any part of the command line before you submit the command by pressing Enter.

When the text to be displayed is longer than a single screen, the output is paused and the phrase —more— is shown at the bottom of the screen. To display the next page of information, press [SPACE]. To display the next line, press [ENTER]. To exit the display and return the CLI to the previous command prompt, press [Q].

To stop the terminal pause (for example, if the CLI commands are scripted), use the **set terminal pause off** command. This setting is not replicated across sessions and therefore needs to be entered at the start of every CLI session, when required. To restart the terminal pause during a session, use the **set terminal pause off** command.

Related Documentation

- Starting a CLI Session on page 5
- Connecting to a DDoS Appliance Using a System Console Connection on page 5
- Changing the Configuration Using the CLI on page 8

Changing the Configuration Using the CLI

The CLI has three principle configuration commands:

- **show**—This is a general-purpose command used to display the current value for various configuration settings. Changes to these configuration settings are performed using the **set** and **remove** commands.
- **set**—This command is used in the majority of cases to configure the system.
- **remove**—This command is used to completely remove a block of configuration (a table entry), such as a server and all its settings. Most individual settings, however, cannot be removed, because they must have a value. Such settings can only be changed from one value to another with the **set** command.

When you make changes to the configuration using the CLI, the pending changes are recorded and applied later (using **apply** command) when instructed by the operator. At any time prior to applying the new configuration, the list of changes to be made can be displayed or cleared.

When the first configuration line is entered, a snapshot of the current configuration is made and all subsequent configuration changes are made against the snapshot configuration. The **apply** command takes the snapshot configuration, applies the configuration changes, and then activates the new configuration. This method avoids the possibility of other users changing the configuration at the same time in such a way that your configuration cannot be applied.

CAUTION: If more than one user attempts to change the configuration simultaneously, then the changes made by the last user are applied, and the other users lose their changes. For this reason, warnings are displayed when two users start to change the configuration at the same time.

Any command used to change the configuration can include the **now** keyword at the end of the input line. Use of this keyword causes the configuration change to be applied immediately.

NOTE: You cannot use the **now** keyword when there are pending changes to be applied.

All CLI commands are case-sensitive and must be entered in lowercase. Most parameters are also case-sensitive; exceptions are detailed in the applicable sections. Table 3 on page 9 describes the basic CLI commands.

Table 3: Basic CLI Commands

Command	Description
apply	Commits and invokes any pending configuration changes.
write	Commits and invokes any pending configuration changes.
discard	It is often helpful when a large amount of configuration has been performed and an error detected, to use the **show pending changes** command prior to **discard**. Then relevant parts of the previous configuration changes can be copied to the terminal. If another user has started editing the configuration, you can also use this method to show the configuration changes you have made. Once the other user has finished, you can then use the **discard** command, paste your changes, and then apply the configuration. This procedure avoids undoing the other user changes.
revert	Reverts the appliance back to the previous configuration. The previous configuration is defined as the configuration prior to the last committed configuration change (with **apply**, or the command suffixed with **now**). WARNING: A **revert** might also undo any configuration changes performed by other users, so care should be taken when you use this command.
now	The **now** option is not a command; rather, it can be appended as the last argument to any CLI command used to change the configuration. When you append the **now** option to a command, that command is not added to the list of pending changes but instead is executed immediately, changing the current running configuration. The **now** option cannot be used if there are any pending changes waiting to be applied. Any such pending changes must either be applied or discarded before a command can use the **now** command.

Related Documentation

- Starting a CLI Session on page 5
- Connecting to a DDoS Appliance Using a System Console Connection on page 5
- Navigating Through the CLI on page 7

show config

Syntax show config

Description Displays the current active configuration of the device.

Sample Output

JS>show config

```
…
set mail server none
set access https all
set access ssh all
set access snmp 192.168.1.221
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show run

Syntax show run

Description Displays the current active configuration of the device.

Sample Output

```
JS>show run
…
set mail server none
set access https all
set access ssh all
set access snmp 192.168.1.221
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show pending changes

Syntax **show pending changes**

Description Displays the list of pending changes for the current user session. The pending changes of other CLI users are not displayed.

Sample Output

```
JS>set access https 192.168.0.0/16
JS>set access ssh 192.168.0.0/16
JS>set access snmp 192.168.0.0/16
JS>show pending changes
set access https 192.168.0.0/16
set access ssh 192.168.0.0/16
set access snmp 192.168.0.0/16

JS>
```

Table 4 on page 12 describes the parameters for the **show pending changes** command.

Table 4: show pending changes Command Parameters

Command	Description
exit	Exits from the CLI.
quit	Quits from the CLI.
context	Synopsis: context newportal The context command allows a user to change between portals, but only if originally logged in to the appliance portal.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

CHAPTER 2

Configurations

This chapter explains access control for DDoS Secure and describes the available advanced configuration commands.

Access Control

The DDoS Secure appliance supports multiple remote access methods. The control of each type of access must be specified with its own **set access** command.

NOTE: Only IPv4 addresses are currently supported.

When you are configuring access control for an appliance, the appliance interprets IP addresses and their networks as classless. You can use both IP host addresses and IP network addresses. You can specify a network address in either network/mask or network/bits format.

Any compound value you enter is parsed as a single entry; there can be no spaces between the entries and the commas that separate them.

Related Documentation

- User Management on page 174
- Starting a CLI Session on page 5
- Changing the Configuration Using the CLI on page 8

show access

Syntax **show access all**

Description Lists the current access settings.

Sample Output

JS>show access all

```
set access https 192.168.1.0/24,192.168.2.3
set access https_juniper yes
set access ssh all
set access ssh_juniper yes
set access snmp 192.168.1.1
```

You can also show individual values by specifying the access type of interest. For example, **JS>show access https**:

JS>show access https

```
set access https 192.168.0.0/16
set access https_juniper yes
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set access https

Syntax **set access https <*IPLIST*|all|none>**

Description Sets the list of IP addresses permitted to connect to the Web-based configuration interface.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set access https_juniper

Syntax **set access https_juniper <yes|no>**

Description Enables/disables the Juniper defined list of public IP addresses permitted to connect to the Web-based configuration interface.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set access ssh

Syntax **set access ssh <*IPLIST*|all|none>**

Description Sets the list of IP addresses permitted to connect through SSH to the command-line configuration interface.

NOTE: The IP address of the client using the command through an SSH connection cannot be removed from the access list. This avoids the possibility of users locking themselves out. If SSH access has to be totally disabled, then this can be done through the CLI over the serial interface or through the Web-based configuration interface.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set access ssh_juniper

Syntax **set access ssh_juniper <yes|no>**

Description Enables/disables the DDoS Secure appliance defined list of appliance public IP addresses permitted to connect to the CLI configuration interface.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set access snmp

Syntax **set access snmp <*IPLIST*|all|none>**

Description Lists the IP addresses permitted to connect to the SNMP management interface for MIB browsing.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Appliance Mode Configuration

This section describes the global appliance operating settings. Table 5 on page 24 describes the appliance mode parameters and their formats.

Table 5: Appliance Mode Parameters

Parameter	Value	Description
hostname	SERVERNAME	Alternative hostname for the appliance, instead of the management IP address.
mode	MODE	Current defense mode. See the *DDoS Secure GUI User Guide* for a full description of operational modes.
hamode	HAMODE	Current high availability mode. See the *DDoS Secure GUI User Guide* for a full description of high availability modes.
autoblockenable	yes|no	If enabled, the appliance automatically blocks all traffic from the worst offending IP addresses exceeding the autoblockrate thresholds.
autoblockratet1	RATE	The minimum required packet drop rate (type 1) before an IP address is added to the blocked list when automatic blocking is enabled. Whenever a packet is dropped, it is classed as a type 1 or a type 2 drop. Typically, RFC violations are of type 1, and decisions/resource consumptions are of type 2. Type 1 rates are usually several orders of magnitude greater than those of type 2.
autoblockratet2	RATE	The minimum required packet drop rate (type 2) before an IP address is added to the blocked list when automatic blocking is enabled.
autoblocksynrst	VALUE	Block IP address if the count exceeds value.

Table 5: Appliance Mode Parameters *(continued)*

Parameter	Value	Description
autoblockfragrate	RATE	If fragment reassembly times out at a rate greater than this, then no fragments are allowed though to the protected IP address in question for at least 5 minutes.
autoblockgetrate	RATE	If a particular tracked IP address keeps accessing a tracked URL and the rate is greater that the defined value, the IP address will get automatically blocked.
autonoblock	IPRANGE|none	Never block these IP addresses.
serverautodetect	yes|no	If enabled, protected IP addresses not previously defined will be protected. If trackindeterminate is enabled, then all IP addresses defined by the appliance portal are allowed to be automatically included. If trackindeterminate is not enabled, then all IP addresses defined in the nonappliance portals are automatically included.
trackindeterminate	yes|no	Used to determine which set of IP addresses can be auto-detected (see serverautodetect).
testenvironment	yes|no	If set, reduces the time that a connection remains in the closed state to 5 seconds from 60 seconds. This is in violation of the RFCs, but might be needed in a testing environment.
priority	PRIORITY	Active-standby priority weighting.
asymrouting	yes|no	If enabled, session state checking is partially relaxed to mitigate potential timing windows when configured in an asymmetric routing environment. This weakens the protection of internal devices.
groupingid	GROUPINGID	Appliances sharing the same grouping ID will replicate state information if configured as active-standby.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show appliance

Syntax show appliance

Description Displays the operating settings of the current appliance.

Sample Output

JS>show appliance

```
set appliance hostname 10.30.12.121 mode logging hamode
 active-standby autoblockenable yes autoblockratet1 200
 autoblockratet2 100 autoblocksynrst 300 autoblockfragrate 10
 autoblockgetrate 300 autonoblock none serverautodetect yes
 trackindeterminate yes testenvironment no allportalsdefending
 no fips_enable no ssl_inspection lowlatency asymrouting no
 priority 0 groupingid 15
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set appliance

Syntax set appliance [hostname <*SERVERNAME*>] [mode <*MODE*>] [hamode <*HAMODE*>] [autoblockenable <yes|no>] [autoblockratet1 <*RATE*>] [autoblockratet2 <*RATE*>] [autoblocksynrst <*VALUE*>] [autoblockfragrate <RATE>] [autoblockgetrate <*RATE*>] [autonoblock <*IPRANGE*|none> [serverautodetect <yes|no>] [trackindeterminate <yes|no>] [testenvironment <yes|no>] [priority <*PRIORITY*>] [asymrouting <yes|no>] [groupingid <*GROUPINGID*>] <*optional-variable*>

Description Sets the global appliance operating settings.

Sample Output

```
JS>set appliance priority 1
JS>apply
JS>show appliance
set appliance hostname 192.168.0.182 mode defending hamode standalone
 autoblockenable yes autoblockratet1 200 autoblockratet2 20 autoblocksynrst 300
 autoblockfragrate 10 autoblockgetrate 300 autonoblock none
 serverautodetect yes trackindeterminate yes testenvironment no
 asymrouting no priority 1 groupingid 15
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Bandwidth and Port Filter Configuration

A DDoS Secure appliance has support for user-defined static packet filter rules. A list of filters associated with a protected IP address and the first filter to be matched in the list is used. If there is no filter match, the traffic is dropped. Each filter consists of a name and a set of options. Filter options are used to define the traffic the appliance allows as well as control the bandwidth used.

Once a filter has been defined, it can be referenced in later parts of the system configuration for use.

Appliance filters are directionless, meaning that they are not specific to a particular direction of traffic. A filter direction is defined when the filter is named in a filter reference, which has a directional context. Additionally, each filter is stateful. Any traffic a filter allows through in one direction will be associated with a session that permits corresponding replies back through in the opposite direction. This is an automatic process, so no filter needs to be defined for the corresponding replies.

NOTE: Once a filter is associated with a connection, the bandwidth controls associated with that filter are applied in both directions.

If multiple servers refer to the same filter, then the bandwidth controls are applied as a sum of all the server traffic matching that filter.

Once a TCP filter session is established, the corresponding traffic is allowed to pass until the session finishes, even if the original permitting filter is altered or replaced with a stricter filter that would otherwise block (any new traffic sessions will be blocked if appropriate). However, UDP, ICMP, and other IP address filter sessions will be blocked as soon as a new filter is applied that would no longer permit that session's traffic. An FTP (port 21) filter also handles the data connections (PORT and PASV) automatically, so no additional filter needs to be defined for FTP.

The appliance filtering system has a logical filter named **default**. This is reserved for use as a default filter where no filter selection has been configured. The filter **default** allows all traffic to pass, with the exception of UDP port 80, and some ICMP types with no bandwidth restrictions.

There are three other predefined filters with the names **broadcast, multicast**, and **redirect**. These filters are applied by default to IP address broadcast, multicast, and redirect traffic, respectively. In contrast to filter **default**, the settings for these predefined filters can be altered.

A filter must already be defined before it can be named within an option that requires a filter. A filter can be named against more than one server configuration or filter aggregation.

Table 6 on page 28 describes the filter parameters and their formats.

Table 6: Filter Parameters

Parameter	Value	Default Value	Description
src_tcp	PORTLIST|all|none	all	The list of tcp source ports permitted for TCP connections.
tcp	PORTLIST|all|none	none	The list of ports permitted for TCP connections.
src_udp	PORTLIST|all|none	all	The list of udp source ports permitted for UDP connections.
udp	PORTLIST|all|none	none	The list of ports permitted for UDP connections.
icmp	ICMPTYPELIST|all|none	none	The list of ICMP types permitted.
icmp6	ICMP6TYPELIST|all|none	none	The list of ICMPv6 types permitted.
otherip	PROTOCOLLIST	none	The list of other IP address protocols (not TCP, UDP, ICMP, or ICMPv6) permitted.

Table 6: Filter Parameters *(continued)*

Parameter	Value	Default Value	Description
countries	COUNTRIES|all|none	all	Defines the countries that are to be permitted by the appliance for this filter. NOTE: The countries test always is applied to the Internet client addresses, not to the protected IP addresses.
aslist	ASLIST|all	all	Defines the AS numbers that are to be permitted by the appliance for this portal. NOTE: The AS numbers test always is applied to the Internet client addresses, not to the protected IP addresses.
networks	IPRANGE|all|none	all	Defines all the networks (up to 4 entries) that are to be permitted by the appliance for this filter. Can be IPv6. NOTE: The networks test always is applied to the Internet client addresses, not to the protected IP addresses.
validpkts	PKTS|U	U	Guaranteed packet rate.
burstpkts	PKTS|U	U	Burstable packet rate.
validspeed	SPEED|U	U	Guaranteed bandwidth.
burstspeed	SPEED|U	U	Burstable bandwidth.
ratelimit-by	filter|internet-ip|protected-ip|match-ips|session	filter	The type of rate limiter matching to create on a filter match.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show filter

Syntax show filter <*FILTERNAME*|all>

Description Displays the settings of the named filters.

Sample Output

JS>show filter test1

```
set filter test1 tcp 80 http 80 udp none icmp none icmp6
 none otherip none countries all networks all aslist all validpkts
 U burstpkts U validspeed U burstspeed U ratelimit-by filter
```

Alternatively, the reserved filter name **all** can be specified to show all defined filters.

JS>show filter all

```
set filter inb-tcp tcp all http 80 udp none icmp none icmp6
 none otherip none countries all networks all aslist all
 validpkts U burstpkts U validspeed U burstspeed U ratelimit-by filter
set filter inb-udp tcp none http none udp 1-79,81-442,444-
 65535 icmp none icmp6 none otherip none countries all
 networks all aslist all validpkts 30K burstpkts 30K validspeed U burstspeed U
 ratelimit-by filter
set filter inb-icmp tcp none http none udp none icmp 0-18
 icmp6 1-4,128-154 otherip none countries all networks all
 aslist all validpkts 1K burstpkts 1K validspeed U burstspeed
 U ratelimit-by filter
set filter inb-other tcp none http none udp none icmp none
 icmp6 none otherip all countries all networks all aslist all
 validpkts 30K burstpkts 30K validspeed U burstspeed U ratelimit-by filter
```

NOTE: The logical filter **default** is not listed. Attempts to use **default**, or any nonexistent filter name as a parameter to the **show filter** command, result in the error message **Not configured**. This error is also displayed when the parameter **all** is used but no filters are defined.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove filter

Syntax **remove filter <*FILTERNAME*|all>**

Description Deletes a specified filter. The specified filter will not be deleted if it is currently assigned to a server. The logical filter **default** cannot be deleted.

Sample Output

```
JS>show filter test1

set filter test1 tcp 80 udp none icmp none icmp6 none otherip none
 countries all networks all aslist all validpkts U burstpkts U
 validspeed U burstspeed U ratelimit-by filter
```

```
JS>remove filter test1
JS>apply
JS>show filter test1
Not configured
```

The **remove filter** command can also be used to delete all filters, as long as none are assigned to a server, by using the reserved filter name **all**. If all the filters cannot be removed, then an error message is returned and none are removed. If all the filters can be safely removed, the user will be prompted for confirmation.

```
JS>show filter all
set filter test1 tcp 80 udp none icmp none icmp6 none otherip none validpkts U
 countries all networks all aslist all burstpkts U validspeed U burstspeed U
 ratelimit-by filter
set filter test2 tcp 80,443 udp none icmp none icmp6 none otherip none
 countries all networks all aslist all validpkts U burstpkts U validspeed U
 burstspeed U ratelimit-by filter
```

```
JS>remove filter all
Are you sure [yes/no]? yes
```

```
JS>apply
JS>show filter all
Not configured
```

NOTE: It is possible to turn off prompting, which can be useful when using automated scripts.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set filter

Syntax

```
set filter <FILTERNAME>
[src_tcp <PORTLIST|all|none>]
[tcp <PORTLIST|all|none>]
[src_udp <PORTLIST|all|none>]
[udp <PORTLIST|all|none>]
[icmp <ICMPTYPELIST|all|none>]
[icmp6 <ICMP6TYPELIST|all|none>]
[otherip <PROTOCOLLIST|all|none>]
[countries <COUNTRIES|all|none>]
[networks <IPRANGE|all|none>]
[aslist <ASLIST|all>]
[validpkts <PKTS>] [burstpkts <PKTS>]
[validspeed <SPEED>] [burstspeed <SPEED>]
[ratelimit-by <filter|internet-ip|protected-ip|match-ips|session>]
```

Description

Creates a new filter entry or to modifies an existing one. At a minimum, a name and one parameter value pair must be specified when using this command. If the name specified does not match an existing filter entry, a new entry is created with that name, and any parameter value pair not specified causes that parameter to be set with the default value. If an entry already exists that matches the name specified then only the parameter value pairs specified are altered.

The following protocol numbers have no effect when used as values with the other IP address parameter, as these protocols are handled separately by their own parameter value pair:

- 1 (ICMP
- 6 (TCP)
- 17 (UDP)
- 58 (ICMPv6)

Sample Output

```
JS>show filter all
set filter inb-tcp tcp all http 80 udp none icmp none icmp6 none otherip none
 countries all networks all aslist all validpkts U burstpkts U validspeed U
 burstspeed U ratelimit-by filter
set filter inb-udp tcp none http none udp 1-79,81-442,444-65535 icmp none
 icmp6  none otherip none countries all networks all aslist all validpkts 30K
 burstpkts 30K validspeed U burstspeed U ratelimit-by filter
set filter inb-icmp tcp none http none udp none icmp 0-18 icmp6 1-4,128-154
 otherip none countries all networks all aslist all validpkts 1K burstpkts 1K
 validspeed U burstspeed U ratelimit-by filter
set filter inb-other tcp none http none udp none icmp none icmp6 none
 otherip all countries all networks all aslist all validpkts 30K
 burstpkts 30K validspeed U burstspeed U ratelimit-by filter
```

```
JS>set filter test1 tcp 80-85,443
JS>set filter test2 udp none icmp 8
JS>apply
```

JS>show filter all

```
set filter test1 tcp 80-85,443 udp none icmp none icmp6 none otherip none
 countries all networks all aslist all validpkts U burstpkts U validspeed U
 burstspeed U ratelimit-by filter
set filter test2 tcp 80,443 udp none icmp 8 otherip none icmp6 none countries
 all networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
 ratelimit-by filter
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

BGP Flow Spec Definitions

DDoS Secure can be used as a BGP Flow Spec injector into an upstream router. The upstream router acts upon these Flow Spec rules (as determined by its configuration). Automatically inserted Flow Spec rules are used to rate-limit specific traffic from the Internet to the DDoS Secure appliance. Rules are automatically added for any IP address that has moved from the Worst Offenders list to the Temporary Black-List list.

Table 7 on page 33 describes the BGP parameters.

Table 7: BGP Parameters

Parameter	Value	Description
ddos_secure	IPADDRESS	The IP address of the DDoS Secure appliance that the BGP Flow Spec injector will run on. For active-standby HA, both management IP addresses need to be defined as separate statements.
our_as	ASNUMBER	Local AS#.
neigh_ip	IPADDRESS	BGP neighbor router IP.
neigh_as	ASNUMBER	Neighbor AS#.
neigh_pass	PASSWORD	Password for secure communications with neighbor.
lowertimer	NUMBER	Length of time before idle BGP Flow Spec rule is dropped.
autoinject	yes|no	If set, automatically injects rules into the router; otherwise, the rules are only displayed in the GUI as Inactive.
ratelimit	SPEED	Rate-limit speed used in the auto-created Flow Spec rules. The default is 100 K.
source	IPNETWORK	Network address that will match the Source IP.

Table 7: BGP Parameters *(continued)*

Parameter	Value	Description
destination	IPNETWORK	Network address that will match the Destination IP. Note that only protected IPs can be defined here, and the entire network must sit in one portal.
protocol	PROTOCOLLIST	List of protocols to match.
srcport	PORTLIST	List of source ports to match (tcp/udp).
dstport	PORTLIST	List of destination ports to match (tcp/udp).
tcpflags	TCPFLAGS	List of TCP flags to match against.
icmpcode	ICMPCODELIST	List of ICMP codes to match (icmp).
icmptype	ICMPTYPELIST	List of ICMP types to match (icmp).
fragment	FRAGMENTLIST	List of fragment types to match.
length	LENGTHLIST	List of packet lengths to match against.
dscp	DSCPLIST	List of DSCP to match against.
action	ACTION	Action to take on Flow Spec rule match.
actionvalue	ACTIONVALUE	Value to apply to action where appropriate.

Related Documentation

- show bgp on page 35
- set bgp peer on page 36
- set bgp flowspec on page 37
- remove bgp on page 38

show bgp

Syntax show bgp <all|peer|flowspec>

Description Displays the current BGP configuration.

Sample Output

JS>show bgp all

```
set bgp peer ddos_secure 192.168.0.189 our_as 65099 neigh_ip 192.168.0.254
 neigh_as 65014 neigh_pass 123456 lowertimer 1000 autoinject no
 ratelimit 100K
```

NOTE: A simple peer (MX Series router) working definition example that matches the DDoS Secure BGP definition above is:

```
routing-options {
    router-id 192.168.0.254;
    autonomous-system 65014;
}
protocols {
    bgp {
        family inet {
            flow {
                no-validate everything;
            }
        }
        authentication-key 123456
        group flow {
            multihop;
            local-preference 100;
            local-address 192.168.0.254;
            export everything;
            peer-as 65099;
            neighbor 192.168.0.189;
        }
    }
}
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set bgp peer

Syntax

set bgp peer ddos_secure <*IPADDRESS*> our_as <*ASNUMBER*> neigh_ip <*IPADDRESS*> neigh_as <*ASNUMBER*> neigh_pass <*PASSWORD*> lowertimer <*NUMBER*> autoinject <yes|no> ratelimit <*SPEED*>

Description

Defines a BGP setup where the defined DDoS Secure appliance acts as a BGP Flow Spec injector. For active-standby HA systems, each DDoS Secure needs a BGP definition, and the upstream router needs to recognize both DDoS Secure as peers.

If autoinject is set to **no** when a BGP Flow Spec rule is dynamically created, DDoS Secure sets it to the **Inactive** state; so that it is not uploaded to the BGP peer. If autoinject is set to **yes** when the BGP FlowSpec rule is created, it is set to the **Active** state and the Flow Spec rule is immediately uploaded to the BGP Peer. Through the GUI, you can easily swap the dynamic Flow Spec rules between Inactive and Active states.

NOTE: If the DDoS Secure is running in the Logging mode, then the dynamic Flow Spec rules are always created as Inactive.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set bgp flowspec

Syntax **set bgp flowspec [source <*IPNETWORK*>] destination <*IPNETWORK*> [protocol <*PROTOCOLLIST*>] [srcport <*PORTLIST*>] [dstport <*PORTLIST*>] [tcpflags <syn|ack|fin|rst|push|urg>] [icmpcode <*ICMPCODELIST*>] [icmptype <*ICMPTYPELIST*>] [fragment <don't|first|is|last|not>] [length <*LENGTHLIST*>][dscp <*DSCPLIST*>] action <accept|discard|mark|redirect|ratelimit|sample|terminal|sample-terminal> [actionvalue <*ACTIONVALUE*>]**

Description Allows you to manually configure the Flow Spec rules that will always be sent to the BGP peer. Only specify the entities that you want to match against. Destination and action are mandatory.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove bgp

Syntax **removebgp <all|peer|flowspec>**

Description Allows you to remove the specified BGP definitions.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Block Country and IP Address Configuration

Table 8 on page 38 describes the block parameters.

Table 8: Block Parameters

Parameter	Value	Description
country	COUNTRIES|all|none	Defines the countries that are to be blocked by the appliance.
cignoreip	IPLIST	Ignores country code blocking for these IP addresses, even though the IP in question is located in that country.
ip	IPRANGE|none	Defines the list of IP address and networks that are to be blocked by the appliance.
as	1 - 65535	Autonomous system number that BGP uses for routing traffic across the Internet.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show block

Syntax show block

Description Displays the current blocked countries and IP addresses.

Sample Output

```
JS>show block

set block country none
set block cignoreip none
set block ip none
set block as none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set block country

Syntax **set block country <*COUNTRIES*|all|none>**

Description Drops all traffic to or from a country for the duration of an attack that originates in that country. Specify a list of countries to block IP addresses from those countries, as tagged by MaxMind. This requires that you periodically update the MaxMind database.

Sample Output

```
JS>set block country USA
JS>apply
JS>show block

set block country USA
set block cignoreip none
set block ip none
set block as none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set block cignoreip

Syntax set block cignoreip <*IPRANGE*|none>

Description Allows access to and from specific, trusted IP addresses from a country while blocking all other traffic to or from that country for the duration of an attack that originates in that country.

Sample Output

JS>set block cignoreip 1.2.3.4
JS>apply
JS>show block

```
set block country USA
set block cignoreip 1.2.3.4
set block ip none
set block as none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set block ip

Syntax **set block ip <*IPRANGE*|none>**

Description Permanently drops all traffic to or from a specific set of IP addresses. You specify the list of IP addresses or networks, separated by commas.

Sample Output

```
JS>set block ip 10.20.0.0/25
JS>apply
JS>show block

set block country USA
set block cignoreip none
set block ip 10.20.0.0/25
set block as none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set block as

Syntax **set block as <*ASLIST*|none>**

Description Permanently drops all traffic to or from a specific AS. You specify the list of AS numbers, separated by commas.

Sample Output

JS>set block as 65001
JS>apply
JS>show block

```
set block country USA
set block cignoreip none
set block ip 10.20.0.0/25
set block as 65001
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Country Code (geoip) Definitions

You can specify country codes for specific IP addresses that override the MaxMind definitions or to categorize pseudo-countries for ease of control of blocks of addresses. You do this by defining the country code with a list of IP addresses and specifying a URL from which to download the IP addresses. These IP addresses are held in a flat file, line-delimited, each line being an IP address, a subnet, or a range of IP addresses.

Several country codes have a special significance:

- -bl—Any IP addresses matching this code are always black-listed.
- -wl—Any IP addresses matching this code are always white-listed.
- -pl—Any IP addresses matching this code are treated as preferred clients.
- -wn—Any IP addresses matching this code are always white-listed, but no logs generated.

The IP address lookup database is built in the following order, with subsequent entries overwriting any previous IP address definitions:

- MaxMind Information
- Bogon list (which contains RFC1918 addresses defined as bogons) http://www.cymru.com/Documents/bogon-bn-agg.txt.
- RFC 1918 addresses
- User definitions specified by geoip entries

Table 9 on page 44 describes the geoip parameters.

Table 9: Geoip Parameters

Parameter	Value	Description
code	COUNTRYCODE	Defines the country code that is to be set.
ip	IPRANGE	Defines the list of IP address and networks that are to be associated with the country code.
freq	FREQUENCY	Frequency at which the URL is checked for updates.
url	URL	Defines the URL containing the list of IP addresses, line-separated, an IP address range per line.
header	HEADER	Matches header definition, including trailing :.
respcode	CODE	HTTP response code to be generated.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show geoip

Syntax show geoip <all|ip|url|megaproxy_ip|megaproxy_url|auto_akamai>

Description Displays the current geoip definition list.

Sample Output

```
JS>show geoip all
No geoip definitions set up
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove geoip

Syntax

remove geoip <all|ip|url|megaproxy_ip|megaproxy_url|auto_akamai>

Description

Deletes the current inspection list.

Sample Output

```
JS>remove geoip all
JS>apply
JS>show geoip all
No geoip definitions set up
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set geoip ip

Syntax **set geoip ip code <*COUNTRYCODE*> ip <*IPRANGE*>**

Description Sets a range of IP addresses to be associated with the given country code. The country codes include -bl (black-list) and -wl (white-list) as described in "Country Code (geoip) Definitions" on page 43.

Sample Output

```
JS>set geoip ip code -bl ip 1.2.3.4
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set geoip url

Syntax **set geoip url code <*COUNTRYCODE*> freq <*FREQUENCY*> url <*URL*>**

Description Updates the country code to use for the list of IP addresses, networks, or IP address range (one entry per line) at the given URL, updated at the given frequency.

Sample Output

```
JS>set geoip url code -wl freq h url http://www.domain.com/white-list.txt
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set geoip megaproxy_ip

Syntax

```
set geoip megaproxy_ip header <HEADER>
respcode <RESPCODE> ip <IPRANGE>
```

Description

Defines a list of IP addresses, networks, or IP address ranges, to be treated as a megaproxy. If the defined header is matched (typically X-forwarded-for:), then the original client is abstracted and used for charm calculations. If the session is to be dropped (for example: original client is blacklisted) then a suitable message is constructed using the specified HTTP response code (for example: 503).

Sample Output

```
JS>set geoip megaproxy_ip header X-Forwarded-For: respcode 503 ip 1.2.3.4-1.2.3.7
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set geoip megaproxy_url

Syntax

```
set geoip megaproxy_url header <HEADER>
respcode <RESPCODE> freq <FREQUENCY> url <URL>
```

Description

Defines a remote URL that contains a list of IP addresses, networks, or IP address ranges, one per line, to be treated as a megaproxy.

If the defined Header is matched (typically X-forwarded-for:), then the original client is abstracted and used for charm calculations. If the session is to be dropped (for example: original client is blacklisted) then a suitable message is constructed using the specified HTTP response code (for example: 503).

The list of IP addresses is updated at the specified frequency.

Sample Output

```
JS>set geoip megaproxy_url header True-Client-IP: respcode 503 freq h url
http://www.domain.com/megaproxy-list.txt
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set geoip auto_akamai

Syntax **set geoip auto_akamai respcode <RESPCODE>**

Description The auto_akamai parameter instructs DDoS Secure to assume that client's traffic that contains the header: true-client-IP: is coming from Akamai, and to treat the client IP address as being a megaproxy.

Sample Output

JS>set geoip url code –bl freq h http://black.list.com/list.txt
JS>set geoip megaproxy_ip header X-Forwarded-For: respcode 503 ip 1.2.3.4
JS>apply
JS>show geoip all

```
JS>set geoip url code -bl freq h url http://black.list.com/list.txt
set geoip megaproxy_ip header X-Forwarded-For: respcode 503 ip 1.2.3.4
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

CHARM Tunables

Changing these values should only be done under the guidance of a DDoS Secure appliance engineer and any changes will affect the charm weighting values. Table 10 on page 51 describes the tunable parameters.

Table 10: Tunable Parameters

Parameter	Value	Default Value	Description
charmgetratebias	BIAS	10	A scalar multiplier for reducing the CHARM score when the URL request rate reaches its limit.
charmconnratebias	BIAS	1	A scalar multiplier for reducing the CHARM score when the new connection request rate reaches its limit.
charmconnbias	BIAS	1	A scalar multiplier for reducing the CHARM score when the current connections reaches its limit.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show tuneable

Syntax **show tuneable [all|default]**

Description Displays the tunable information.

Sample Output

```
JS>show tuneable all
set tuneable charmgetratebias 10
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove tuneable

Syntax remove tuneable all

Description Deletes the current tunable definitions.

Sample Output

```
JS>remove tuneable all
JS>apply
JS>show tuneable all
tuneable disabled
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set tuneable

Syntax **set tuneable <charmgetratebias|charmconnratebias|charmconnbias> <*BIAS*>**

Description Allows specific charm biases to be modified.

Sample Output

```
JS>set tuneable charmgetratebias 10
JS>apply
JS>show tuneable all
set tuneable charmgetreatebias 10
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Chassis Definitions

One version of the DDoS Secure appliance is provided in a chassis configuration with multiple blades where each blade is effectively an appliance in its own right, but can share a common VIP for management access. Associated with this is the ability to configure the appliance as a BGP trigger router for rerouting of traffic. Table 11 on page 54 describes the chassis parameters.

Table 11: Chassis Parameters

Parameter	Value	Description
ip	IPADDRESS	IP address to be used.
netmask	NETMASK	Netmask to be used.
ddos_secure	IPADDRESS	The appliance blade acting as trigger router.
our_as	ASNUMBER	Local AS #.
neigh_ip	IPADDRESS	BGP neighbor router.
neigh_as	ASNUMBER	Neighbor AS #.
neigh_pass	PASSWORD	Password to secure communications with neighbor.
comm_as	ASNUMBER	Trigger community AS #.
comm_no	NUMBER	Trigger community number.

Table 11: Chassis Parameters *(continued)*

Parameter	Value	Description
lowertimer	NUMBER	Length of time below rerouting rate before dropping the trigger route.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show chassis

Syntax **show chassis <all|vip|blade|bgp|reroute>**

Description Displays the current chassis configuration.

Sample Output

```
JS>show chassis all
set chassis blade ip 192.168.0.6
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set chassis vip

Syntax **set chassis vip ip <IPADDRESS> netmask <NETMASK>**

Description Defines the common VIP by which the DDoS Secure appliance chassis can be accessed.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set chassis blade

Syntax **set chassis blade ip <IPADDRESS>**

Description Defines the management access for the individual blade within the chassis. This is also used to define the IP addresses of DDoS Secure appliances that are participating in BGP rerouting.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set chassis bgp

Syntax

```
set chassis bgp ddos_secure <IPADDRESS>
our_as <ASNUMBER>
neigh_ip <IPADDRESS> neigh_as <ASNUMBER>
neigh_pass <PASSWORD> comm_as <ASNUMBER>
comm_no <NUMBER> lowertimer <NUMBER>
```

Description

Defines the BGP setup where the defined DDoS Secure appliance is going to act as a trigger router for injecting BGP routes. This is used in conjunction with the reroute definitions for a portal, which are applied on a per-protected-IP-address basis, to inject or withdraw a route.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set chassis reroute

Syntax set chassis reroute ip <IPADDRESS>

Description Sets a permanent injection of the defined protected IP address into the BGP trigger routing tables.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Disable RFC Testing

It is possible to disable some of the RFC compliancy checking, but this does provide a security risk for the protected servers. Not all the RFC checking can be configured. Table 12 on page 60 describes the disable parameters.

Table 12: Disable Parameters

Parameter	Value	Description
all	yes|no	Disables all the optional RFC checking.
badudppacket_no_data	yes|no	Disables checking for UDP packets with no data.
tcpattack_nodata	yes|no	Disables no data transfer alerting.
blockedstate_invalidstate	yes|no	Disables invalid TCP state alerting.
blockedstate_nostate	yes|no	Disables no TCP state alerting.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show disabled

Syntax show disabled

Description Displays the current RFC disabled state.

Sample Output

```
JS>show disabled
Nothing disabled
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set disabled

Syntax set disabled <all|badudppacket_nodata|tcpattack_nodata| blockedstate_invalidstate|blockedstate_nostate> <yes|no>

Description Specifies RFC checks to be disabled.

Sample Output

```
JS>set disabled all yes
JS>apply
JS>show disabled

set disabled unknownsession_nostate yes
 unknownsession_invalidstate yes badudppacket_nodata yes
 tcpattack_nodata yes badippacket_reflectedroute yes
 tcpattack_url_ratelimited yes udpattack_dns_ratelimited yes
 udpattack_sip_ratelimited yes badtcppacket_chksum yes
 tcpattack_http_format yes unknownsession_reflective yes
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Date and Time

Table 13 on page 62 describes the date and time parameters and their formats.

Table 13: Date and Time Parameters

Parameter	Value	Description
timenow	TIMESTRING	The date and time.
timezone	TIMEZONE	The time zone for displaying date and time.
ntp	IPLIST|none	NTP server(s) with which to synchronize.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show clock

Syntax show clock

Description Displays the current time, time zone and NTP server configured.

Sample Output

JS>show clock

```
set clock timenow 2003-01-15T15:26:27
set clock timezone Europe/London
set clock ntp none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set clock timenow

Syntax set clock timenow <*TIMESTRING*>

Description Sets the system clock. It is important to set the system time zone to the correct value before adjusting the clock time. This is because the **set clock timenow** command assumes that all time values entered are offset from UTC time by the local time zone. If the local time is configured while the time zone is set to a region with a different time offset from UTC, the clock will effectively be wrong by the number of hours separating the current local time zone from the system set time zone. This difference will clear when the system time zone value is corrected.

NOTE: This command is applied immediately without having to use the **now** parameter or using the **apply** command.

Sample Output

```
JS>show clock timenow
set clock timenow 2013-11-14T14:21:27
JS>set clock timenow 2013-11-14T14:00:00
JS>apply
JS>show clock timenow
set clock timenow 2013-11-14T14:00:03
JS>set clock timenow “14 nov2013 15:00:00”
JS>apply
JS>show clock timenow
set clock timenow 2013-11-14T15:00:03
JS>set clock timenow “14-nov-13 16:00:00”
JS>apply
JS>show clock timenow
set clock timenow 2013-11-14T16:00:03
JS>set clock timenow “nov 14 17:00:00 2013”
JS>apply
JS>show clock timenow
JS>set clock timenow 2013-11-14T17:00:02
JS>apply
```

Related Documentation

- **set clock timezone on page 65**
- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set clock timezone

Syntax **set clock timezone <*TIMEZONE*>**

Description Sets the time zone of the appliance. A complete list of valid time zones can be displayed using the **show timezones** command.

Sample Output

```
JS>show clock
set clock timenow 2003-08-13T21:01:11
set clock timezone Europe/London
set clock ntp none

JS>set clock timezone Europe/Paris
JS>apply
JS>show clock
set clock timenow 2003-08-13T22:01:22
set clock timezone Europe/Paris
set clock ntp none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set clock ntp

Syntax **set clock ntp <*IPLIST*|none>**

Description Defines the NTP server or servers. A DDoS Secure appliance unit can also take advantage of an NTP server to help maintain a more accurate value for the time. The **set clock ntp** command can be used to define one or more NTP servers to be used for synchronizing the time. Time synchronizations are performed every hour but if the difference between the appliance local clock and the NTP server clock is greater than a few minutes. It is recommended that the **set clock timenow** command is used first to bring the two clocks closer together.

Sample Output

```
JS>set clock ntp 128.118.25.3,140.162.8.25,130.88.200.98
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show timezones

Syntax

show timezones

Description

Displays a complete list of time zones supported by the DDoS Secure appliance. Since the list is long, the system automatic paging takes over before the first line of the answer scrolls off the top of the display. It is important to note that time zone values are case-sensitive.

Sample Output

JS>show timezones

```
Available timezones:
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
 -- more –
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Debug Options

The debug options are used to aid in the diagnosis of suspicious traffic handling by a DDoS secure appliance unit. When enabled, the DDoS secure appliance generates detailed logs, but this can be at the expense of top end performance. The debug options should only be enabled at the suggestion of DDoS secure appliance support staff. By default, **worstoffenders** and **autoblacklist** are enabled, as they tend not to create too high a loading.

Table 14 on page 68 describes the Debug Option parameters and their formats.

Table 14: Debug Option Parameters

Parameter	Value	Description
bandwidth	yes|no	Bandwidth throttle debugging.
packetrate	yes|no	Packet Rate debugging.
blockedprotocol	yes|no	Blocked protocol debugging.
blockedstate	yes|no	Blocked state debugging.
attackip	yes|no	IP attack debugging.
attacktcp	yes|no	TCP attack debugging.
attackudp	yes|no	UDP attack debugging.
attackicmp	yes|no	ICMP attack debugging.
attackotherip	yes|no	Other IP attack debugging.
attackfragment	yes|no	Fragment attack debugging.

Table 14: Debug Option Parameters *(continued)*

Parameter	Value	Description
badippacket	yes|no	Bad IP packet debugging.
badtcppacket	yes|no	Bad TCP packet debugging.
badudppacket	yes|no	Bad UDP packet debugging.
badicmppacket	yes|no	Bad ICMP packet debugging.
badotherippacket	yes|no	Bad other IP packet debugging.
overloadedip	yes|no	Server stall debugging.
all	yes|no	This is a special option and represents the combination of all the above combinations.
worstoffenders	yes|no	Log Worst Offenders to main log file.
autoblacklist	yes|no	Log Auto-Blacklist to main log file.

show debugging

Syntax **show debugging**

Description Displays the current debugging options.

Sample Output

```
JS>show debugging

set debugging bandwidth no packetrate no blockedprotocol no blockedstate no
 attackip no attacktcp no attackudp no attackicmp no attackotherip no
 attackfragment no badippacket no badtcppacket no badudppacket no
 badicmppacket no badotherippacket no overloadedip no worstoffenders yes
 autoblacklist yes incidentdetail no
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set debugging

Syntax **set debugging <*PARAMETER*> <*VALUE*> [...]**

Description Sets the <*PARAMETER*> <*VALUE*> pair is taken from the debug option parameters.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

External Authenticators

There are two types of external authenticators, as well as the local password file, for authentication. If an external authenticator is defined and enabled, then the password checking order is external (RADIUS), then external (TACACS+), if both the options fail, then local is used. Table 15 on page 72 describes the external authenticator type details.

Table 15: External Authenticator Types

Parameter	Value	Description
radius	RADIUS	Requires an external RADIUS server, which holds the user authentication records.
tacacs+	TACACS+	Requires an external TACACS+ server, which holds the user authentication records.

NOTE: TACACS+ is not available by default.

Table 16 on page 72 describes the external authenticator parameters and their formats.

Table 16: External Authenticator Parameters

Parameter	Value	Description
server	IPADDRESS	The IP address of the server.
backup	IPADDRESS|none	Alternative server IP address.
secret	SECRET	The secret need to encrypt/decrypt the authentication session.
enabled	yes|no	Whether the authenticator is enabled or not.
port	PORT	The port the RADIUS server is listening on.
protocol	TPROTOCOL	TACACS+ protocol.
service	TSERVICE	TACACS+ service.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- User Management on page 174
- Access Control on page 18

show auth

Syntax show auth

Description Displays the list of the authenticator definitions.

Sample Output

JS>show auth

```
set auth radius server 192.168.0.3 backup none port 1812 secret secret
 enabled yes
set auth tacacs+ server 192.168.0.3 backup none secret secret-1 protocol
 lcp service DDoS Secure appliance enabled no
```

Users with operator permissions will be shown the secrets masked out.

JS>show auth

```
set auth radius server 192.168.0.3 backup none port 1812 secret xxxxxxxx
 enabled yes
set auth tacacs+ server 192.168.0.3 backup none secret xxxxxxxx protocol
 lcp service juniper enabled no
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set auth

Syntax

set auth radius server <*IPADDRESS*>
[backup <*IPADDRESS*>|none> secret <*SECRET*> [port <*PORT*>]
set auth tacacs+ server <*IPADDRESS*>
[backup <*IPADDRESS*>|none>] secret <*SECRET*>
protocol <*TPROTOCOL*> service <*TSERVICE*>

Description

Modifies any parameters of an authenticator definition.

A user has to be defined on the DDoS Secure appliance (with a password) before this command can be used to either connect to the GUI or to connect through SSH. We recommend that you set at least one known local password so that it is possible to authenticate to the appliance in an emergency when the external authenticator is not available.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Filter Aggregation Configuration

Servers require a list of one or more filters when determining what traffic to allow. This list is searched for the first match and then used. To aid you in configuring these lists, filter aggregations are used to define a list of up to seven filters. A filter aggregation might refer to a (previously defined) filter aggregation to extend the list.

A filter aggregation must already be defined before it can be named within an option that expects a filter or filter aggregation. A filter aggregation can be named against more than one server configuration or filter aggregation.

Table 17 on page 75 describes the filter aggregation parameters and their formats.

Table 17: Filter Aggregation Parameters

Parameter	Value	Default Value	Description
filtera	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterb	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterc	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterd	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filtere	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterf	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterg	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.

Table 18 on page 75 describes the filter fixed value and its format.

Table 18: Filter Fixed Value Formats

Parameter Value	Description
-undefined-	Entry not in use.

show fagg

Syntax show fagg <FILTERNAME|all>

Description Displays the settings of the named filter aggregation.

Sample Output

JS>show fagg web-agg

```
set fagg web-agg filtera web filterb default filterc -undefined- filterd
 -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
```

Alternatively, the reserved filter name **all** can be specified to show all defined filters.

JS>show fagg all

```
set fagg web-agg filtera web filterb default filterc -undefined- filterd
 -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
set fagg example-agg filtera default filterb -undefined- filterc
 -undefined- filterd -undefined- filtere -undefined- filterf
 -undefined- filterg -undefined-
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove fagg

Syntax remove fagg <*FILTERNAME*|all>

Description Deletes a specified filter aggregation. The specified filter aggregation will not be deleted if it is currently assigned to a server.

Sample Output

```
JS>show fagg web-agg

set fagg web-agg filtera web filterb default filterc -undefined- filterd
 -undefined- filtere -undefined- filterf -undefined- filterg
 -undefined-
```

```
JS>remove fagg web-agg
JS>apply
JS>show fagg web-agg
Not configured
```

The **remove fagg** command can also be used to delete all filter aggregations, as long as none are assigned to a server, by using the reserved filter name **all**. If all the filter aggregations cannot be removed then an error message is returned and none are removed. If all the filter aggregations can be safely removed, the user will be prompted for confirmation.

```
JS>show fagg all

set fagg web-agg filtera web filterb default filterc -undefined- filterd
 -undefined- filtere -undefined- filterf -undefined- filterg
 -undefined-
set fagg example-agg filtera default filterb -undefined- filterc -undefined-
 filterd -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
```

```
JS>remove fagg all
Are you sure [yes/no]? yes
```

```
JS>apply
JS>show fagg all
Not configured
```

NOTE: It is possible to turn off prompting which can be useful when using automated scripts.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set fagg

Syntax set fagg <*FILTERNAME*> [filtera <*FILTERNAME*|-undefined->]
[filterb <*FILTERNAME*|-undefined->]
[filterc <*FILTERNAME*|-undefined->]
[filterd <*FILTERNAME*|-undefined->]
[filtere <*FILTERNAME*|-undefined->]
[filterf <*FILTERNAME*|-undefined->]
[filterg <*FILTERNAME*|-undefined->]

Description Creates a new filter aggregation entry or modifies an existing one. At a minimum, a name and one parameter value pair must be specified when using the command. If the name specified does not match an existing filter entry, a new entry is created with that name and any parameter value pair not specified causes that parameter to be set with the default value. If an entry already exists that matches the name specified then only the parameter value pairs specified are altered.

Sample Output

JS>show fagg all

```
set fagg web-agg filtera web filterb default filterc -undefined- filterd
 -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
set fagg example-agg filtera default filterb -undefined- filterc
 -undefined- filterd -undefined- filtere -undefined- filterf -undefined-
 filterg -undefined-
```

JS>set fagg web-agg filterg webplus
JS>apply
JS>show fagg all

```
set fagg web-agg filtera web filterb default filterc -undefined- filterd
 -undefined- filtere -undefined- filterf -undefined- filterg webplus
set fagg example-agg filtera default filterb -undefined- filterc -undefined-
 filterd -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Layer 7 Inspection

It is possible to inspect certain Layer 7 requests, and give weightings (negative CHARM bias) to specific requests to discourage repeated access to these requests. This bias is also added to the Worst Offenders Resource Usage average rate, so it must have a value that is less than **autoblockratet2** (see set appliance). Currently, inspection of HTTP URLs and DNS queries is supported. Matching is defined by:

- The matching of the entire request, including parameters.
- The matching of the initial part of the request, which can possibly include some parameters.
- The use of Basic Regular Expression syntax.
- The use of Extended Regular Expression syntax. To prevent unexpected matches—for example, a match on any / in the URL that does not indicate a homepage—use the ^ and $ anchors.

Where possible, we recommend that you use matching methods 1 and 2 for performance reasons.

Table 19 on page 79 describes the show inspect parameters.

Table 19: Show Inspect Parameters

Parameter	Value	Example	Description
url_match	all|*STRING*	http://a.b.c/file	Exact match of an HTTP query.
url_regex	all|*REGEX*	http://a.*/file	Regular expression match of an HTTP request.
dns_match	all|*STRING*	www.juniper.net?A	Match on a DNS query.
dns_regex	all|*REGEX*	*?ANY	Regular expression match on a DNS query.
sip_match	all|*STRING*	sip:123456@1.2.3.4	Exact match on a SIP query.
sip_regex	all|*REGEX*	sip:8@1.2.3.4	Regex match on a SIP query.
sip_eregex	all|*EREGEX*	sip:8@1.2.3.4	Save, but use extended regex format.

show inspect

Syntax

show inspect
url_match <all|*STRING*>|url_prefix <all|*STRING*>|
url_regex <all|*REGEX*>|url_eregex <all|EREGEX> |
dns_match <all|*STRING*>|dns_prefix <all|*STRING*>|
dns_regex <all|*REGEX*>|dns_eregex <all|*EREGEX*> |
sip_match <all|*STRING*>|sip_prefix <all|*STRING*>|
sip_regex <all|*REGEX*>|sip_eregex <all|*EREGEX*> |
sip_eregex <all|*REGEX*>|sip_eregex <all|*EREGEX*> >

Description

Displays the current inspection list and weighting.

Sample Output

```
JS>show inspect all
Inspect disabled
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove inspect

Syntax

remove inspect
url_match <all|*STRING*>|url_prefix <all|*STRING*>|
url_regex <all|*REGEX*>|url_eregex <all|*EREGEX*>|
dns_match <all|*STRING*>|dns_prefix <all|*STRING*>|
dns_regex <all|*REGEX*>|dns_eregex <all|*EREGEX*>|
sip_match <all|*STRING*>|sip_prefix <all|*STRING*>|
sip_regex <all|*REGEX*>|sip_eregex <all|*EREGEX*>

Description

Deletes the current inspection list.

Sample Output

```
JS>remove inspect all
JS>apply
JS>show inspect all
Inspect disabled
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set inspect

Syntax

```
set inspect
url_match <STRING>|url_prefix <STRING>|
url_regex <REGEX>|url_eregex <EREGEX> |
dns_match <STRING>|dns_prefix <STRING>|
dns_regex <REGEX>|dns_eregex <EREGEX> |
dns_match <STRING>|sip_prefix <STRING>|
dns_regex <REGEX>|sip_eregex <EREGEX> |
<bl|-bl|wl|BIAS> >
```

Description Allows for the checking of specific Layer 7 requests by different inspection methods.

Sample Output

```
JS>set inspect url_regex ^/index.asp$ 10
JS>apply
JS>show inspect all
set inspect url_regex "^www.site.com/index.asp$" 10 order 0
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Logging Thresholds

A DDoS secure appliance uses a set of values known as Create Thresholds to determine the rate, for each defense type, at which the user would like an incident record to be created. The thresholds define at what rate packets must be dropped before the incident is created. An incident is considered closed when the drop rate remains below the defined threshold for longer than the specified incident timeout.

Create thresholds are mirrored by three other sets of thresholds. The first of these is the offenders threshold set, which determines the rate at which packets must be dropped for an individual client IP address to warrant addition to the worst offenders table. The second set is the alert thresholds set, which determines when an alert e-mail or SNMP trap is sent, as well as being logged in the regular log file. The third is the view thresholds set, which determines the rates at which packets must be dropped before the corresponding incidents are listed on the Web UI. This last set is effectively a viewing filter to limit the display of incidents to those of most interest.

The following commands describe how to examine and change these threshold values, as well as ignore certain types of attack completely if desired:

- **show threshold create**
- **show threshold offenders**

- show threshold alert
- show threshold view

Table 20 on page 83 describes the logging threshold types.

Table 20: Logging Threshold Types

Parameter	Description
create	Thresholds associated with the creation of incidents.
offenders	Thresholds associated with entry into the worst offenders table.
alert	Thresholds associated with the sending of e-mail alerts.
view	Thresholds associated with the viewing/display of incidents.

Table 21 on page 83 describes the logging threshold parameters and their formats.

Table 21: Logging Threshold Parameters

Parameter	Value	Description
bandwidthenable	yes|no	Enable/disable logging dropped packets exceeding bandwidth threshold.
bandwidthrate	THRESHOLD	Threshold for logging dropped packets exceeding bandwidth threshold.
packetrateenable	yes|no	Enable/disable logging dropped packet rate packets.
packetraterate	THRESHOLD	Threshold for logging dropped packet rate packets.
blockedprotocolenable	yes|no	Enable/disable logging dropped packets which do not match the appropriate filter.
blockedprotocolrate	THRESHOLD	Threshold for logging dropped packets which do not match the appropriate filter.
blockedstateenable	yes|no	Enable/disable logging dropped packets because they were out of state.
blockedstaterate	THRESHOLD	Threshold for logging dropped packets because they were out of state.
attackipenable	yes|no	Enable/disable logging dropped packets because they constitute an IP attack.
attackiprate	THRESHOLD	Threshold for logging dropped packets because they constitute an IP attack.

Table 21: Logging Threshold Parameters *(continued)*

Parameter	Value	Description
attacktcpenable	yes|no	Enable/disable logging dropped packets because they constitute a TCP attack.
attacktcprate	THRESHOLD	Threshold for logging dropped packets because they constitute a TCP attack.
attackudpenable	yes|no	Enable/disable logging dropped packets because they constitute a UDP attack.
attackudprate	THRESHOLD	Threshold for logging dropped packets because they constitute a UDP attack.
attackicmpenable	yes|no	Enable/disable logging dropped packets because they constitute an ICMP attack.
attackicmprate	THRESHOLD	Threshold for logging dropped packets because they constitute an ICMP attack.
attackotheripenable	yes|no	Enable/disable logging dropped packets because they constitute an attack not covered by the above 4 cases.
attackotheriprate	THRESHOLD	Threshold for logging dropped packets because they constitute an attack not covered by the above 4 cases.
attackfragmentenable	yes|no	Enable/disable logging dropped packets because they constitute a fragment attack.
attackfragmentrate	THRESHOLD	Threshold for logging dropped packets because they constitute a fragment attack.
badippacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid IP packet.
badippacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid IP packet.
badtcppacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid TCP packet.
badtcppacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid TCP packet.
badudppacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid UDP packet.
badudppacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid UDP packet.

Table 21: Logging Threshold Parameters *(continued)*

Parameter	Value	Description
badicmppacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid ICMP packet.
badicmppacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid ICMP packet.
badotherippacketenable	yes|no	Enable/disable logging dropped packets because they are invalid and not covered by ip, tcp, udp and icmp cases.
badotherippacketrate	THRESHOLD	Threshold for logging dropped packets because they are invalid and not covered by ip, tcp, udp and icmp cases.
overloadedipenable	yes|no	Enable/disable logging packets because of the overloaded ip condition.
overloadediprate	THRESHOLD	Threshold for logging packets because of the overloaded ip condition.
allenable	yes|no	Enable/disable logging dropped packets for all attack types. This is a quick way of enabling or disabling everything.
allrate	THRESHOLD	Sets the threshold for logging all attack packets to be the same.
autoadjust	yes|no	Enable/disable automatic adjusting of create thresholds, so that the number of generated incidents per day is limited to being between 10 and 100 per type per day. NOTE: Only valid for create.

show threshold view

Syntax **show threshold view**

Description Displays the current incident view threshold configuration.

Sample Output

JS>show threshold view

```
set threshold view bandwidthenable yes bandwidthrate 100
set threshold view packetrateenable yes packetraterate 100
set threshold view blockedprotocolenable yes blockedprotocolrate 100
set threshold view blockedstateenable yes blockedstaterate 100
set threshold view attackipenable yes attackiprate 100
set threshold view attacktcpenable yes attacktcprate 100
set threshold view attackudpenable yes attackudprate 100
set threshold view attackicmpenable yes attackicmprate 100
set threshold view attackotheripenable yes attackotheriprate 100
set threshold view attackfragmentenable yes attackfragmentrate 100
set threshold view badippacketenable yes badippacketrate 100
set threshold view badtcppacketenable yes badtcppacketrate 100
set threshold view badudppacketenable yes badudppacketrate 100
set threshold view badicmppacketenable yes badicmppacketrate 100
set threshold view badotherippacketenable yes badotherippacketrate 100
set threshold view overloadedipenable yes overloadediprate 100
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show threshold create

Syntax show threshold create

Description Displays the current incident create threshold configuration.

Sample Output

JS>show threshold create

```
set threshold create autoadjust yes
set threshold create bandwidthenable yes bandwidthrate 10
set threshold create packetrateenable yes packetraterate 10
set threshold create blockedprotocolenable yes blockedprotocolrate 10
set threshold create blockedstateenable yes blockedstaterate 10
set threshold create attackipenable yes attackiprate 10
set threshold create attacktcpenable yes attacktcprate 10
set threshold create attackudpenable yes attackudprate 10
set threshold create attackicmpenable yes attackicmprate 10
set threshold create attackotheripenable yes attackotheriprate 10
set threshold create attackfragmentenable yes attackfragmentrate 10
set threshold create badippacketenable yes badippacketrate 10
set threshold create badtcppacketenable yes badtcppacketrate 10
set threshold create badudppacketenable yes badudppacketrate 10
set threshold create badicmppacketenable yes badicmppacketrate 10
set threshold create badotherippacketenable yes badotherippacketrate 10
set threshold create overloadedipenable yes overloadediprate 10
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show threshold offenders

Syntax **show threshold offenders**

Description Displays the worst offenders recording thresholds.

Sample Output

JS>show threshold offenders

```
set threshold offenders bandwidthenable yes bandwidthrate 10
set threshold offenders packetrateenable yes packetraterate 10
set threshold offenders blockedprotocolenable yes blockedprotocolrate 10
set threshold offenders blockedstateenable yes blockedstaterate 10
set threshold offenders attackipenable yes attackiprate 10
set threshold offenders attacktcpenable yes attacktcprate 10
set threshold offenders attackudpenable yes attackudprate 10
set threshold offenders attackicmpenable yes attackicmprate 10
set threshold offenders attackotheripenable yes attackotheriprate 10
set threshold offenders attackfragmentenable yes attackfragmentrate 10
set threshold offenders badippacketenable yes badippacketrate 10
set threshold offenders badtcppacketenable yes badtcppacketrate 10
set threshold offenders badudppacketenable yes badudppacketrate 10
set threshold offenders badicmppacketenable yes badicmppacketrate 10
set threshold offenders badotherippacketenable yes badotherippacketrate 10
set threshold offenders overloadedipenable no overloadediprate 10
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show threshold alert

Syntax **show threshold alert**

Description Displays the current incident alert threshold configurations.

Sample Output

JS>show threshold alert

```
set threshold alert bandwidthenable yes bandwidthrate 100
set threshold alert packetrateenable yes packetraterate 100
set threshold alert blockedprotocolenable yes blockedprotocolrate 100
set threshold alert blockedstateenable yes blockedstaterate 100
set threshold alert attackipenable yes attackiprate 100
set threshold alert attacktcpenable yes attacktcprate 100
set threshold alert attackudpenable yes attackudprate 100
set threshold alert attackicmpenable yes attackicmprate 100
set threshold alert attackotheripenable yes attackotheriprate 100
set threshold alert attackfragmentenable yes attackfragmentrate 100
set threshold alert badippacketenable yes badippacketrate 100
set threshold alert badtcppacketenable yes badtcppacketrate 100
set threshold alert badudppacketenable yes badudppacketrate 100
set threshold alert badicmppacketenable yes badicmppacketrate 100
set threshold alert badotherippacketenable yes badotherippacketrate 100
set threshold alert overloadedipenable no overloadediprate 100
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set threshold

Syntax

set threshold <create|view|alert|offenders>
<*PARAMETER*> <*VALUE*> [...]

Description

Sets the <*PARAMETER*> <*VALUE*> pair is taken from the logging threshold parameter.

The threshold is the number of packets dropped per second while the attack is in progress. Once this threshold rate is exceeded, then the attack is logged as an incident. Create rates are calculated on a per-protected-server basis. The offender rates are calculated on a per-client basis.

NOTE: If the view/alert threshold is set lower than the create threshold for a particular defense type, then it will only trigger when the Incident has been created.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show incidents

Syntax **show incidents**

Description Displays the incident timeout, lifetime, and warning threshold. An incident is closed when the packet rate has been below the create threshold for the specified number of timeout minutes, or the incident has been open for more than the specified lifetime minutes.

An Incident is only alerted on if the Incident has been above the alert threshold for at least the configured threshold number of seconds. Table 22 on page 91 describes the incident parameters.

Sample Output

```
JS>show incidents
set incidents timeout 5 lifetime 60 threshold 60
```

Table 22: Incident Parameters

Parameter	Value	Description
timeout	TIMEOUT	How long an incident drop rate must be below the create threshold before the incident is closed (in minutes).
lifetime	LIFETIME	How long an Incident can live for (in minutes).
threshold	THRESHOLDTIME	Length of time an item is above the threshold before an event triggers (in seconds).
logrefresh	LOGREFRESHTIME	Length of time an incident refresh update for Structured Log (secs).

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set incidents

Syntax

set incidents [timeout <*TIMEOUT*>] [lifetime <*LIFETIME*>]
[threshold <*THRESHOLDTTIME*>]
[logrefresh <*LOGREFRESHTIME*>]

Description

Sets the incident timeout, lifetime, logrefresh, or threshold times.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

MAC Gateway Configuration

A DDoS Secure appliance unit operates at both the Ethernet layer and the Internet Protocol layers. Defense is managed at the Ethernet layer based on a list of gateways, which are tracked by Ethernet MAC addresses. The Ethernet addresses discovered can be those of routers and firewalls, or they can be those of individual hosts, but they are all treated the same way. Ethernet addresses detected on the appliance Internet interface are classified as Internet gateways, and the addresses detected on the appliance protected interface are classified as protected gateways. Gateways are detected automatically and each is configured with the default maximum bandwidth allowed until configured otherwise.

Table 23 on page 92 describes the gateway types.

Table 23: Gateway Types

Gateway Type	Description
protected	All gateways detected or specified connected to the protected interface.
Internet	All gateways detected or specified connected to the Internet interface.

Table 24 on page 92 describes the gateway parameters and their formats.

Table 24: Gateway Parameters

Parameter	Value	Description
tospeed	SPEED	The maximum speed that data can be sent to the gateway. If the data trying to be sent to the gateway exceeds this speed then bandwidth defense will be applied.
topkts	PKTS	The maximum packet rate that can be sent to the gateway. If the packet rate to the gateway exceeds this setting then packet rate defense will be applied.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show gateway

Syntax

show gateway <internet|protected> <*MAC*|all|autodetected>
show gateway <all>

Description

Displays the selected gateway configuration

The second parameter is used to refine the selection of the gateways still further. The value **all** is used to show all defined gateways and their configuration. A value of ***<MAC>*** displays the gateway with the specified MAC address along with its configuration. The value **auto-detected** displays only the MAC address of any auto-detected gateways. Auto-detected gateways are not part of the actual configuration and thus only MAC addresses are listed.

Sample Output

JS>show gateway all

```
set gateway internet 00:90:27:EA:BF:96 tospeed 0 topkts 10K
set gateway protected 01:02:03:04:05:06 tospeed 100M topkts 37.2K
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove gateway

Syntax **remove gateway <internet|protected> <*MAC*|all|autodetected>**

Description Removes the defined gateway from the configuration.

NOTE: When the value **all**, or **autodetected**, is used with the remove gateway command, the user is prompted to verify the selection. This prompting can be turned off, which may be of use for scripted configurations.

When **autodetected** is used, the command is applied immediately without having to use the **now** parameter or the **apply** command.

Sample Output

```
JS>remove gateway internet all
Are you sure [yes/no]? yes
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set gateway

Syntax **set gateway <internet|protected> <*MAC*> [tospeed <*SPEED*>] [topkts <*PKTS*>]**

Description Adds a new gateway to the configuration, or changes the settings of a gateway already defined in the configuration. The two parameters determine when bandwidth defense and packet rate defense should be activated. By default, the packet rate defense maximum threshold value **<*PKTS*>** is 25% of the maximum packet rate of the bandwidth threshold value **<*SPEED*>** when composed entirely of minimum-size packets (this percentage is increased for speeds less than 8M, and 100% for speeds less than 2M). A higher value may be needed for a busy gateway heavily used by chat software, but many gateways start to suffer from performance problems when over 50% of their rated bandwidth limit is used to carry small packets alone.

Sample Output

```
JS>set gateway internet 00:01:02:03:04:05 tospeed 10M
JS>apply
JS>show gateway internet 00:01:02:03:04:05
set gateway internet 00:01:02:03:04:05 tospeed 10M topkts 3720
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Mail Reporting

A DDoS Secure appliance unit can send incident alerts or daily reports through e-mail. These are configurable on a per-portal basis. Table 25 on page 96 describes the e-mail parameters.

Table 25: Mail Parameters

Parameter	Value	Description
to	EMAILADDRESSES	The e-mail address to which the alert or daily report is to be sent. Comma-separated addresses can be specified.
from	EMAILADDRESS	The e-mail address from which the alert or daily report appears to come.
server	IPADDRESS|none	The IP address of the SMTP server to which the alert or daily report is to be forwarded.
wsserver	IPADDRESS|none	The IP address through which the appliance is accessed, which may be different from the actual appliance management IP address.

Table 25: Mail Parameters *(continued)*

Parameter	Value	Description
dailystats	yes|no	If set, a daily summary of statistics is e-mailed.
weeklystats	yes|no	If set, a weekly summary of statistics is e-mailed.
monthlystats	yes|no	If set, a monthly summary of statistics is e-mailed.
cluster	yes|no	If set, a cluster daily summary is sent out as well.
alerts	yes|no	If set, incident alerts are e-mailed out at a rate no faster than specified by alert interval.
alertinterval	ALERTINTERVAL	This is the minimum amount of time (in minutes) between two e-mail alerts, acting as a rate limiter. Each e-mail can contain information about multiple incidents.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show mail

Syntax show mail

Description Displays the current daily e-mail configuration.

Sample Output

JS>show mail

```
set mail server none dailystats yes weeklystats yes monthlystats yes alerts no
 nullsender yes cluster no alertinterval 5
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set mail

Syntax

set mail [to <*EMAILADDRESSES*>] [from <*EMAILADDRESS*>]
[server <*IPADDRESS*|none>] [wsserver <*IPADDRESS*|none>]
[dailystats <yes|no>] [weeklystats <yes|no>]
[monthlystats <yes|no>] [alerts <yes|no>]
[cluster <yes|no>] [alertinterval <*ALERTINTERVAL*>]

Description

E-mail is not sent unless, at a minimum, the to, from, and server parameter values are defined. The server IP address cannot be configured without valid to and from parameters. The to and from parameters may be configured previously or along with the server IP address. Below is an example warning given when attempting to set a server IP address without valid to and from parameters.

Sample Output

JS>set mail server 192.168.0.10

```
mail: from <EMAILADDRESS>: missing
mail: to <EMAILADDRESS>: missing
```

JS>apply

```
Nothing to apply!
```

JS>set mail server 192.168.0.10 to test@yourdomain.com
from jdds@yourdomain.com
JS>apply
JS>show mail
set mail server 192.168.0.10 from jdds@yourdomain.com
to test@yourdomain.com dailystats yes weeklystats yes monthlystats yes
alerts no nullsender yes cluster no alertinterval 5

Once a parameter value has been set, that value will be used until changed. It is not necessary to set all the values every time one of them needs to be changed. The server address can be set to none to disable e-mails from being sent.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Network Configuration

Each DDoS Secure appliance has four network interfaces, along with a common definition, as described in Table 26 on page 99.

Table 26: Interface Types

Interface Name	Description
Management	The management interface, for the appliance management.
Protected	The protected interface, connected to the protected hosts on the LAN.

Table 26: Interface Types *(continued)*

Interface Name	Description
Internet	The Internet interface, connected to hosts on the rest of the LAN or the Internet.
Datashare	The data share interface, used to share state and incident information between the appliances. This interface might not be available on all hardware configurations.
Global	For setting parameters that are common to both Internet and protected interfaces.

Table 27 on page 100 lists all the possible configuration parameters. However, not all interface type will accept them. IP addresses can only be configured on the management and data share interfaces as they are the only interfaces on an appliance unit that have an active TCP/IP stack.

Table 27: Interface Parameters

Parameter	Value	Description
hwid	HARDWARE-ID	The hardware ID of the appliance. If this parameter is specified then any following parameters are ignored if the hardware ID specified does not match that of the appliance. This parameter is always shown when displaying the configuration because interface configuration is unique to an individual appliance.
ip	IPADDRESS	The IPv4 address of the appliance management or data share interface.
netmask	NETMASK	The netmask of the appliance management or data share interface.
gateway	IPADDRESS|none	The default gateway of the appliance management interface. Specify none to clear the default gateway.
linkmode	LINKMODE	The link mode of the interface.
fcmode	FCMODE	The flow control mode of the interface.
mtu	MTU_SIZE	The MTU size (default 1500) for traffic flowing between the Internet and protected interfaces.
lfpt	<yes|no>	Whether a link failure on one (Internet/protected) interface of the appliance is to be passed through to the other side by dropping the transmitter.
cdp	<yes|no>	Whether all the interfaces are to generate CDP packets or not.
portpair1	<yes|no>	Multiple fail-safe cards are available. The first fail-safe card is known as portpair1.

Table 27: Interface Parameters *(continued)*

Parameter	Value	Description
portpair2	<yes|no>	Multiple fail-safe cards are available. The second fail-safe card is known as portpair2.
trackvlans	<yes|no>	If set, different VLANs will cause different stateful sessions even if they have the same IP addresses and ports.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- MAC Gateway Configuration on page 92

show interface

Syntax show interface

Description Displays the network interface configuration. Each interface can be configured with or without the unique appliance hardware ID (always shown on display output), that enables the automatic generation of a common configuration to be shared with multiple DDoS Secure appliance units. It also allows each unit to have customized network interface configurations when the hardware ID is included.

Sample Output

```
JS>show interface
set interface management hwid 00:01:02:03:04:05 ip 192.168.30.30
 netmask 255.255.255.0 gateway 192.168.30.1 linkmode auto fcmode full
set interface protected hwid 00:01:02:03:04:05 linkmode auto fcmode none
set interface internet hwid 00:01:02:03:04:05 linkmode auto fcmode none
set interface datashare hwid 00:01:02:03:04:05 ip 10.1.1.30
 netmask 255.255.255.0 linkmode auto fcmode none mtu 1500
set interface global mtu 1500 cdp yes lfpt no trackvlans no portpair1 yes
 portpair2 yes
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set interface management

Syntax

set interface management [hwid <*HARDWARE-ID*>] [ip <*IPADDRESS*>] [netmask <*NETMASK*>] [gateway <*IPADDRESS*|none>] [linkmode <*LINKMODE*>] [fcmode <*FCMODE*>]

Description

Sets the basic TCP/IP configuration and link mode of the management interface. The TCP/IP options are required for remote network management of the DDoS Secure appliance. One or more parameters can be configured at the same time, with or without the addition of the **hwid** parameter. But, the **hwid** parameter cannot be specified alone. Even if only one parameter is set, all the current settings are shown when the configuration is displayed.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set interface datashare

Syntax

set interface datashare [hwid <*HARDWARE-ID*>]
[ip <*IPADDRESS*|none] [netmask <*NETMASK*>]
[linkmode <*LINKMODE*>] [fcmode <*FCMODE*>] [mtu <*MTU_SIZE*>]

Description

Sets the basic TCP/IP configuration and link mode of the data share interface. If the IP address is set to **none**, then the data share interface will not be used. One or more parameters can be configured at the same time, with or without the addition of the **hwid** parameter. But, the **hwid** parameter cannot be specified alone. Even if only one parameter is set, all the current settings are shown when the configuration is displayed.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set interface protected

Syntax

set interface protected [hwid <*HARDWARE-ID*>]
linkmode <*LINKMODE*> [fcmode <*FCMODE*>]

Description

Sets the link mode of the protected interface. Not all link mode values can be supported depending on the DDoS Secure appliance model. The specification of **hwid<*HARDWARE-ID*>** is optional but helps avoid misconfiguration when sharing configuration files between the appliances. The **hwid** option and its value are always included when the configuration is displayed or saved. The **hwid** option cannot be specified alone.

If this interface spans multiple interfaces (WS-3G), then all subinterfaces will be set to the same specification. Load sharing across the multiple interfaces will be done by the switch connected to the protected interface. Any 802.3ad packets are passed through to the Internet interface for onward transmission, so that the Internet and protected switches can set up their own link aggregation. Any packet received on one of the subinterfaces will be sent out of the corresponding subinterface. The upstream/downstream switch must be configured for lag/teaming mode and load share appropriately.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set interface internet

Syntax **set interface internet [hwid <*HARDWARE-ID*>] linkmode <*LINKMODE*> [fcmode <*FCMODE*>]**

Description Sets the link mode of the Internet interface. Not all link mode values may be supported depending on the DDoS Secure appliance model. The specification of **hwid <*HARDWARE-ID*>** is optional but helps avoid misconfiguration when sharing configuration files between the appliances. The **hwid** option and its value are always included when the configuration is displayed or saved. The **hwid** option cannot be specified alone.

If this interface spans multiple interfaces (WS-3G), then all subinterfaces will be set to the same specification. Load sharing across the multiple interfaces will be done by the switch connected to the Internet interface. Any 802.3ad packets are passed through to the protected interface for onward transmission so that the Internet and protected switches can set up their own link aggregation. Any packet received on one of the subinterfaces will be sent out of the corresponding subinterface. The upstream/downstream switch must be configured for lag/teaming mode and load share appropriately.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set interface global

Syntax

set interface global mtu <*MTU_SIZE*> lftp <yes|no>
cdp <yes|no> trackvlans <yes|no>
portpair1 <yes|no> portpair2 <yes|no>

Description

Sets the common definition for traffic flowing between the Internet and protected interfaces, which port pairs are enabled, and whether CDP packets are to be generated or not on all interfaces.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show dns

Syntax show dns

Description Shows the current DNS configuration.

Sample Output

```
JS>show dns
set dns forwarder 192.168.0.3
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set dns

Syntax **set dns forwarder <*IPLIST*>**

Description Sets the IP address of the DNS server(s), to forward any DNS queries to.

Table 28 on page 109 lists the DNS configuration parameter.

Table 28: DNS Parameter

Parameter	Value	Description
forwarder	IPLIST	One or more IP addresses, which acts as the DNS server.

Sample Output

```
JS>set dns forwarder 192.168.0.3
JS>show dns
set dns forwarder 192.168.0.3
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove route

Syntax **remove route <all|*IPNETWORK*>**

Description Removes additional routing.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show route

Syntax **show route <all|*IPNETWORK*>**

Description Shows the additional routing.

Sample Output

```
JS>show route all
Not configured
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set route

Syntax **set route cidr <*IPNETWORK*> gateway <*IPADDRESS*>**

Description Sets additional routing incase the default gateway is insufficient to access different IP addresses. It is not normally required, as the default gateway is usually sufficient.

Table 29 on page 112 lists the route configuration parameter.

Table 29: Route Parameter

Parameter	Value	Description
cidr	IPNETWORK	A classless Internet domain routing definition.
gateway	IPADDRESS	The gateway for the classless Internet domain.

Sample Output

```
JS>show route all
Not configured
```

```
JS>set route cidr 192.168.1.0/24 gateway 192.168.0.1
JS>apply
JS>show route all
set route cidr 192.168.1.0/24 gateway 192.168.0.1
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

NetFlow

The DDoS Secure appliance is capable of sending netflow packets (Version 9: RFC 3954) to a NetFlow collector for data analysis and reporting. Table 30 on page 112 describes the netflow parameters.

Table 30: NetFlow Parameters

Parameter	Value	Description
ip	IPLIST|IPMULTI|none	The IP address to which webtrends messages will be sent.
port	PORT	The port number that the netflow collector is listening on.
templatep	TEMPLATEP	Retransmit the netflow templates after transmitting this number of netflow packets, or the templatem timeout has expired.

Table 30: NetFlow Parameters *(continued)*

Parameter	Value	Description
templatem	TEMPLATEM	Retransmit the netflow templates after this time in minutes, or when templatep packets have been transmitted.
flowflush	FLOWFLUSH	Generate a netflow record for a flow after this time in minutes.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show netflow

Syntax show netflow

Description Displays the current netflow logging configuration.

Sample Output

JS>show netflow

```
set netflow ip 192.168.1.99 port 9996 templatep 1000 templatem 60 flowflush 1
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set netflow

Syntax

set netflow [ip <*IPLIST*|*IPMULTI*|none>] [port <*PORT*>] [templatep <*TEMPLATEP*>] [templatem <*TEMPLATEM*>] [flowflush <*FLOWFLUSH*>]

Description

Sets the netflow collector to be configured to receive data on the correct port, and the DDoS Secure appliance IP address to be configured as a valid source address.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Preferred Clients and Whitelisting Configuration

Table 31 on page 115 describes the preferred parameters and their formats.

Table 31: Preferred Parameters

Parameter	Value	Description
clients	IPRANGE|none	Defines the client IP addresses (on the Internet side of the appliance) get preferential treatment by giving them a charm boost.
countries	COUNTRIES|none	Defines which countries get preferential treatment by giving them a charm boost.
default	IPRANGE|none	Defines the client IP addresses (on the Internet side of the appliance) always get the default charm scoring.
whitelisted	IPRANGE|none	Defines the client network (on the Internet side of the appliance) that can be used for pen-testing. All packets coming from a white-listed network are passed through as if the appliance was operating in logging. There is therefore no protection for the protected IP addresses by the appliance for any packets coming from this network address.
whitenolog	IPRANGE|none	Defines the client network (on the Internet side of the appliance) that can be used for pen-testing. All packets coming from a white-listed network are passed through as if the appliance was operating in logging. There is therefore no protection for the protected IP addresses by the appliance for any packets coming from this network address. Note: None of this traffic is logged.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show preferred

Syntax show preferred
[all|clients|countries|whitenolog|whitelisted|default]

Description Displays the current clients and pen-test networks.

Sample Output

JS>show preferred all

```
set preferred clients none
set preferred whitenolog 192.168.213.0/24,172.16.166.0/24
set preferred whitelisted none
set preferred default none
set preferred countries none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set preferred clients

Syntax **set preferred clients <*IPRANGE|none*>**

Description Sets the preferred clients. It is possible that there may be some client addresses that need preferential treatment by the DDoS Secure appliance charm engine when the protected servers are under load/attack conditions. By specifying these IP addresses in the preferred clients list, these IP addresses will get a boost when calculated. If these IP addresses do not perform properly, packets from these IP addresses may still get dropped.

Sample Output

```
JS>set preferred clients 192.168.10.1
JS>apply
JS>show preferred clients
set preferred clients 192.168.10.1
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set preferred countries

Syntax **set preferred countries <*COUNTRIES*|none>**

Description Specifies the countries in the preferred countries list. It is possible that there may be some countries that need preferential treatment by the DDoS Secure appliance charm engine when the protected servers are under load/attack conditions. By specifying these countries in the preferred countries list, the IP addresses from these countries will get a charm boost when is calculated. If the IP addresses from these countries misbehave badly, packets from these IP addresses may still get dropped.

Sample Output

```
JS>set preferred countries GBR
JS>apply
JS>show preferred countries
set preferred countries GBR
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set preferred whitelist

Syntax **set preferred whitelisted <*IPRANGE*|none>**

Description Sets the preferred whitelist. If there is a client network that needs to pen-test servers through the DDoS Secure appliance, even if the IP addresses are specified as **preferred clients**, it is likely that the pen-test traffic will get blocked. The **preferred whitelist** option effectively makes the appliance engine run in logging mode for the defined whitelisted network addresses. For all other IP addresses, the appliance engine will run in the defined appliance mode.

Sample Output

```
JS>set preferred whitelisted 10.20.0.0/25
JS>apply
JS>show preferred whitelisted
set preferred whitelisted 10.20.0.0/25
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set preferred whitenolog

Syntax **set preferred whitenolog <*IPRANGE*|none>**

Description Sets the preferred whitelist for which no logging will be performed. If there is a client network that needs to pen-test servers through the DDoS Secure appliance, even if the IP addresses are specified as **preferred clients**, it is likely that the pen-test traffic will get blocked. The **preferred whitenolog** option effectively makes the appliance engine run in logging mode for the defined whitelisted network addresses. For all other IP addresses, the appliance engine will run in the defined appliance mode.

NOTE: Any misbehaving activity to/from these IP addresses will not get logged anywhere.

Sample Output

```
JS>set preferred whitenolog 10.30.0.0/25
JS>apply
JS>show preferred whitenolog
set preferred whitelisted 10.30.0.0/25
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set preferred default

Syntax **set preferred default <IPRANGE|none>**

Description Sets the preferred default list. It is possible that there may be some client addresses that always need default treatment by the DDoS Secure appliance engine when the protected servers are under load/attack conditions. By specifying these IP addresses in the preferred default list, these IP addresses will always get the default when is calculated. If these IP addresses misbehave badly, packets from these IP addresses may still get dropped.

NOTE: Examples could be website availability monitors.

Sample Output

```
JS>set preferred default 192.168.20.1
JS>apply
JS>show preferred default
set preferred clients 192.168.20.1
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Portals

It is possible to specify blocks of addresses (networks and/or single IP addresses, known as *portals*), which can be managed separately by designated users. This gives the ability for customers, clients or business groups to be able to manage what appliance does for their portal. Any user that has full managerial access can override these portal configurations. The master portal is known as a DDoS Secure appliance.

The sum of all the values of the portals (excluding the master) cannot exceed that of the master portal, with the exception of the burst values, which individually cannot exceed that of the master portal.

Table 32 on page 122 describes the portal parameters and their format.

Table 32: Portal Parameters

Parameter	Value	Description
ip	IPRANGE|all	The list of protected IP addresses.
vlan	VLANSDEF	The list of VLANs/MPLS definitions to track as opposed to IP addresses.

Table 32: Portal Parameters *(continued)*

Parameter	Value	Description
validpkts	PKTS|U	Guaranteed packet rate.
burstpkts	PKTS|U	Burstable packet rate. Over this rate triggers an Incident.
validspeed	SPEED|U	Guaranteed bandwidth.
burstspeed	SPEED|U	Burstable bandwidth. Over this rate triggers an Incident.
filters	FILTERS	The number of configurable filters.
rerouteminpkts	PKTS	Rerouting is dropped when IP address is below this packet rate.
reroutemaxpkts	PKTS	Rerouting is potentially triggered when above this packet rate.
rerouteminspeed	SPEED	Rerouting is dropped when IP address is below this bandwidth.
reroutemaxspeed	SPEED	Rerouting is potentially triggered when above this bandwidth.
protected	PROTECTED	The number of configurable protected IP addresses.

Related Documentation

- Access Control on page 18
- MAC Gateway Configuration on page 92
- Shares Configuration on page 146
- **show portal on page 124**
- **remove portal on page 125**
- **set portal on page 126**

show portal

Syntax show portal <PORTALNAME|all>

Description Displays the settings of the named portal.

Sample Output

JS>show portal test1

```
set portal test1 ip 10.0.0.0/24 validpkts 3720 burstpkts 3720 validspeed 10M
 burstspeed 50M filters 31 rerouteminpkts 1K reroutemaxpkts 50K rerouteminspeed
 20M reroutemaxspeed 1G protected 16
```

Alternatively the reserved portal name **all** can be specified to show all defined portals.

JS>show portal all

```
set portal DDoS Secure appliance ip all validpkts 37.2K burstpkts 37.2K
 validspeed 100M burstspeed 100M filters 991 rerouteminpkts 1K
 reroutemaxpkts 50K rerouteminspeed 20M reroutemaxspeed 1G protected 1
set portal example ip 10.0.0.0/24 validpkts 3720 burstpkts 3720 validspeed 10M
 burstspeed 50M filters 31 rerouteminpkts 1K reroutemaxpkts 50K rerouteminspeed
 20M reroutemaxspeed 1G protected 16
```

Related Documentation

- Portals on page 122
- **remove portal on page 125**
- **set portal on page 126**
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove portal

Syntax

```
remove portal <PORTALNAME|all>
```

Description

Deletes a specific portal. This command can also be used to delete all current portals. To do this the parameter value all is used instead of a portal name. When deleting all portals the command will ask for confirmation.

NOTE: It is possible to disable the prompting, which can be useful for automated scripts.

Related Documentation

- Portals on page 122
- **show portal on page 124**
- **set portal on page 126**
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set portal

Syntax

```
set portal <PORTALNAME> [ip <IPRANGE|all>|vlan <VLANSDEF>]
[validpkts <PKTS>] [burstpkts <PKTS>]
[validspeed <SPEED>] [burstspeed <SPEED>]
[filters <FILTERS>] [rerouteminpkts <PKTS>]
[reroutemaxpkts <PKTS>] [rerouteminspeed <SPEEED>]
[reroutemaxspeed <SPEEED>] [protected <PROTECTED>]
```

Description Creates a new portal or modifies an existing one.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8
- **show portal on page 124**
- **remove portal on page 125**

Portal Operational Mode Configuration

This section describes the operational mode of a portal.

Table 33 on page 126 describes the operational mode parameters and their formats.

Table 33: Operational Mode Parameters

Parameter	Value	Default Value	Description
mode	MODEPORTAL	defending	Current defense mode of the portal. This can be defending or logging.
countries	COUNTRIES|all	all	Defines the countries that are to be permitted by the appliance for this portal. NOTE: The countries test always is applied to the Internet client addresses, not to the protected IP addresses.
aslist	ASLIST|all	all	Defines the AS numbers that are to be permitted by the appliance for this portal. NOTE: The AS numbers test always is applied to the Internet client addresses, not to the protected IP addresses.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show operation

Syntax show operation

Description Displays the current operational mode of the portal.

Sample Output

```
JS>show operation
set operation mode defending countries all aslist all
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set operation

Syntax set operation mode <*MODEPORTAL*> countries <*COUNTRIES*|all> aslist <*ASLIST*|all>

Description Sets the operational mode of the portal.

Sample Output

```
JS>set operation mode logging
JS>apply
JS>show operation
set operation mode logging countries all aslist all
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Portal Defense Configuration

Table 34 on page 128 describes the portal defense parameters and their formats. An example for a portal could be a load balancer with multiple VIPs. Portal defense could then be used to protect this load balancer from overload.

Table 34: Portal Defense Parameters

Parameter	Value	Description
backlog	BACKLOG|auto-BACKLOG	The TCP backlog setting. Refer to the *DDoS Secure GUI User Guide* for further details.
connections	CONNECTIONS|auto-CONNECTIONS	The maximum number of connections. Refer to the *DDoS Secure GUI User Guide* for further details.
connrate	CONNRATE|auto-CONNRATE	The maximum connection rate. Refer to the *DDoS Secure GUI User Guide* for further details.
gets	GETS|auto-GETS	The maximum concurrent number of active GET/HEAD/POST that a server can handle at once. An example is IIS ASP thread count.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show portaldefense

Syntax show portaldefense

Description Displays the portal defense configuration.

Sample Output

```
JS>show portal defense
set portaldefense backlog U connections U connrate U gets U
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set portaldefense

Syntax

set portaldefense
[backlog <*BACKLOG*|auto-*BACKLOG*>]
[connections <*CONNECTIONS*|auto-*CONNECTIONS*>]
[connrate <*CONNRATE*|auto-*CONNRATE*>]
[gets <*GETS*|auto-*GETS*>]

Description Sets the portal defense. If all parameters are not present when defining the portal defense then any unspecified parameters are automatically set to those of the default server.

Sample Output

```
JS>set portaldefense backlog 10000 connections U connrate U gets U
JS>apply
JS>show portaldefense
set portaldefense backlog 10000 connections U connrate U gets U
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Protected IP Configuration

Table 35 on page 130 describes the protected IP address parameters and their format.

Table 35: Protected IP Address Parameters

Parameter	Value	Description
name	PROTECTEDNAME	The text name of the protected IP address. This parameter is ignored when defining settings for the default protected IP address.
backlog	BACKLOG|auto-BACKLOG	The TCP backlog setting. Refer to the *DDoS Secure GUI User Guide* for further details.
connections	CONNECTIONS|auto-CONNECTIONS	The maximum number of connections. Refer to the *DDoS Secure GUI User Guide* for further details.
connrate	CONNRATE|auto-CONNRATE	The maximum connection rate. Refer to the *DDoS Secure GUI User Guide* for further details.
gets	GETS|auto-GETS	The maximum concurrent number of active GET/HEAD/POST that a protected IP address can handle at once. An example is IISs ASP thread count.
infilter	FILTERNAME|default	The filter used for inbound connections.

Table 35: Protected IP Address Parameters *(continued)*

Parameter	Value	Description
outfilter	FILTERNAME	The filter used for outbound connections.
sendtcprejects	yes|no	Send TCP rejects for a TCP connection that does not match any filters.
soap	yes|no	Look for Soap Action headers to differentiate URLs.
fragsdisabled	yes|no	Specifies whether fragments are allowed for this protected IP address.
mode	MODEIP	Specifies the mode that net protected IP address is running under.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show protected

Syntax **show protected <*IPADDRESS*|all|default|indeterminate|broadcast|multicast|redirect|autodetected>**

Description Displays the specified protected IP address configuration.

Sample Output

JS>show protected all

```
set protected default backlog auto-1000 connections auto-1000
 connrate auto-1000 gets auto-1000 infilter inbound outfilter
 outbound sendtcprejects no soap no fragsdisabled no patgw no mode defending
set protected multicast backlog auto-1000
 connections auto-1000 connrate auto-1000 gets auto-1000 infilter multicast
 outfilter multicast sendtcprejects no soap no fragsdisabled no patgw no
 mode defending
set protected broadcast backlog auto-1000 connections auto-1000
 connrate auto-1000 gets auto-1000 infilter broadcast
 outfilter broadcast sendtcprejects no soap no fragsdisabled no patgw no
 mode  defending
set protected indeterminate backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter default outfilter default sendtcprejects no
 soap no fragsdisabled no patgw no mode defending
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove protected

Syntax **remove protected <*IPADDRESS*|all|autodetected>**

Description Deletes the specified protected IP address. The <*IPADDRESS*> field should have a value that matches an existing defined protected IP address, an auto-detected protected entry is not considered a defined protected IP address. If the IP address used does not match any of the existing defined protected IP addresses, the command is ignored.

It is also possible to delete all the defined protected IP addresses. The command **remove protected all** deletes all configured protected IP addresses but prompts for confirmation before the command is accepted. The default protected parameters are not altered by the use of the value **all**. The default, indeterminate, multicast, broadcast, and redirect protected IP address settings cannot be removed.

NOTE: When the value **all**, or **autodetected** is used with the remove protected command the user is prompted if they are sure. This prompting can be turned off, which may be of use for scripted configurations.

When **autodetected** is used, the command is applied immediately without having to use the **now** parameter or issue the **apply** command.

Sample Output

JS>remove protected all
```
Are you sure [yes/no]? yes
```

JS>show protected all
```
set protected default backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter inbound outfilter outbound sendtcprejects
 no soap no fragsdisabled no patgw no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter multicast outfilter multicast
 sendtcprejects no soap no fragsdisabled no patgw no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter broadcast outfilter broadcast
 sendtcprejects no soap no fragsdisabled no patgw no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter default outfilter default sendtcprejects
 no soap no fragsdisabled no patgw no mode defending
set protected 10.50.1.1 backlog 1000 connections 5000 connrate 100
 gets U infilter default outfilter default sendtcprejects yes
 soap no fragsdisabled no patgw no mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100
 gets U infilter default outfilter default sendtcprejects yes
 soap no fragsdisabled no patgw no mode defending
```

JS>remove server 10.50.1.1
JS>apply
JS>show protected all

```
set protected default backlog auto-1000 connections auto-1000 connrate
```

```
 auto-1000 gets auto-1000 infilter inbound outfilter outbound
 sendtcprejects no soap no fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter multicast outfilter multicast
 sendtcprejects no soap no fragsdisabled no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter broadcast outfilter broadcast
 sendtcprejects no soap no fragsdisabled no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter default outfilter default
 sendtcprejects no soap no fragsdisabled no mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100
 gets U infilter default outfilter default sendtcprejects yes soap
 no fragsdisabled no mode defending
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set protected

Syntax

set protected
<*IPADDRESS*|default|indeterminate|multicast|broadcast>
[name <*PROTECTEDNAME*>] [backlog <*BACKLOG*|auto-*BACKLOG*>]
[connections <*CONNECTIONS*|auto-*CONNECTIONS*>]
[connrate <*CONNRATE*|auto-*CONNRATE*>]
[gets <*GETS*|auto-*GETS*>]
[infilter <*FILTERNAME*|default>]
[outfilter <*FILTERNAME*|default>]
[sendtcprejects <yes|no>] [soap <yes|no>]
[fragsdisabled <yes|no>] [mode <*MODEIP*>]

Description

Sets the protected IP address. If all parameters are not present while defining a new protected IP address then any unspecified parameters are automatically set to those of the default protected IP address.

Sample Output

JS>show protected all

```
set protected default backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter inbound outfilter outbound
 sendtcprejects no soap no fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter multicast outfilter multicast
 sendtcprejects no soap no fragsdisabled no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter broadcast outfilter broadcast
 sendtcprejects no soap no fragsdisabled no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter default outfilter default sendtcprejects
 no soap no fragsdisabled no mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100 gets U
 infilter default outfilter default sendtcprejects yes soap no
 fragsdisabled no mode defending
```

JS>set server 10.50.1.1 infilter default outfilter default
JS>apply
JS>show protected all

```
set protected default backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter inbound outfilter outbound
 sendtcprejects no soap no fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter multicast outfilter multicast
 sendtcprejects no soap no fragsdisabled no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter broadcast outfilter broadcast sendtcprejects
 no soap no fragsdisabled no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets auto-1000 infilter default outfilter default
 sendtcprejects no soap no fragsdisabled no mode defending
set protected 10.50.1.1 backlog auto-1000 connections auto-1000 connrate
 auto-1000 gets U infilter default outfilter default
 sendtcprejects yes soap no fragsdisabled no mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100
```

```
gets U infilter default outfilter default sendtcprejects yes soap no
fragsdisabled no mode defending
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Proxy Server

If the DDoS Secure appliance needs to get update information through a URL, then the http traffic may have to go through a proxy server to get to the Internet. Table 36 on page 136 describes the proxy server parameters.

Table 36: Proxy Server Parameters

Parameter	Value	Description
proxyip	IPADDRESS|none	The IP address of the proxy server.
proxyport	PORT	The port number that the proxy server is listening on.
proxyuser	USERNAME|none	The user for authenticating to the proxy server.
proxypassword	PASSWORD	The password for the user for authenticating to the proxy server.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show proxy

Syntax show proxy

Description Displays the current proxy server configuration.

Sample Output

```
JS>show proxy
set proxy proxyip 192.168.1.99 proxyport 8080
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set proxy

Syntax set proxy [proxyip <*IPADDRESS*|none>] [proxyport <*PORT*>] [proxyuser <*USERNAME*|none>] [proxypassword <*PASSWORD*>]

Description Sets the current proxy server configuration.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Pseudol3 Configuration

The pseudol3 commands are used to configure the interfaces, networks and routes for the L3 or L2/L3 split modes of operation.

Layer 3: Configure IP/subnets for both the Internet and Protected interfaces as well as a default gateway route for layer 3 functionality. Additional interface aliases and routes can also be defined.

Layer 2/3: This mode splits a network in two and acts as an ARP Man-In-The-Middle. The local subnet must be defined as well as the default gateway route. Additional networks/routes can also be defined.

NOTE: Any IP addresses/routes configured for Layer 3 are not added to the Linux network stack. This means that these IP addresses are not available for ping from any external device. Also, the ping command is unable to ping IP addresses connected to (or routed through) the Internet or Protected.

Table 37: Pseudo Layer 2 and Layer 3 Parameters

Parameter	Value	Description
interface	internet|protected	The interface to which the IP/prefix is assigned.
ip/prefixlen	IP/PREFIXLEN	The IP and prefix length assigned to this interface.
cidr	IPNETWORK	The subnet which is part of the L2/L3 split network.
cidr	IPNETWORK|default|default-ipv4	The subnet for the route to be added.
gateway	IPADDRESS	The gateway for the subnet.

Related Documentation

- Starting a CLI Session on page 5

- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show pseudol3

Syntax **show pseudol3<interface|network|route|all>**

Description Displays the pseudol3 configuration information. The sections can be divided by interface/network/route, or **all** can be displayed.

L2/L3 (Split Network)

JS>show pseudol3 all

```
set pseudol3 network cidr 192.168.1.0/24
set pseudol3 route cidr 192.168.1.0/24 gateway 192.168.1.1
```

JS>show pseudol3 interface

No pseudo layer 3 local interface definitions set up.

JS>show pseudol3 network

```
set pseudol3 network cidr 192.168.1.0/24
```

JS>show pseudol3 route

```
set pseudol3 route cidr 192.168.1.0/24 gateway 192.168.1.1
```

L2 Example

JS>show pseudol3 all

```
set pseudol3 interface located internet ip/prefixlen 192.168.1.230/24
set pseudol3 interface located protected ip/prefixlen 192.168.0.1/24
set pseudol3 route cidr default-ipv4 gateway 192.168.1.1
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set pseudol3 interface

Syntax set pseudol3 route cidr <*IPNETWORK*|default|default-ipv4> gateway <*IPADDRESS*>

Description Assigns a given IP address (with prefix for the subnet) to either the Internet or protected interfaces. This is only used for Layer 3 mode.

Sample Output

```
JS>set pseudol3 interface located internet ip/prefixlen 192.168.1.200/24
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set pseudol3 network

Syntax **set pseudol3 network cidr <*IPNETWORK*>**

Description Adds a network to the L2/L3 (Split Network) mode. This is not compatible with Layer 3 mode.

Sample Output

```
JS>set pseudol3 network cidr 192.168.0.0/24
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set pseudol3 route

Syntax **set pseudol3 route cidr <IPNETWORK|default|default-ipv4>gateway <*IPADDRESS*>**

Description Adds a route entry for the L3 mode.

Sample Output

```
JS>set pseudol3 route cidr default gateway 192.168.1.1
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove pseudol3 all

Syntax **remove pseudol3 all**

Description Removes any pseudol3 configuration.

Sample Output

```
JS>remove pseudol3 all
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove pseudol3 interface

Syntax **remove pseudol3 interface**

Description Removes all pseudol3 interface settings. This will disable layer3 operation.

Sample Output

```
JS>remove pseudol3 interface
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove pseudol3 route

Syntax **remove pseudol3 route**

Description Removes all pseudol3 route settings.

Sample Output

JS>remove pseudol3 route

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Remote Alerts, Reports, and Logging

The DDoS Secure appliance currently supports a number of methods for remote alerts, reports, and logs. Incident alerts can be sent remotely either using SNMP traps, or through e-mail. Daily reports can also be sent remotely by e-mail. Additionally, continuous log data can be sent to a remote syslog server, structured syslog server, or netFlow collector.

This topic describes how to configure the specific settings needed to enable the above forms of remote messaging. This topic does not, however, cover the configuration of event triggers that would then result in incident logs or alerts. These associated settings are covered in the logging threshold topic.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Shares Configuration

This section describes the configuration setting for sharing information between DDoS Secure appliances, other than those working in an active-standby relationship. Table 38 on page 146 describes the share parameters and their formats.

Table 38: Share Parameters

Parameter	Value	Description
gateway	IPADDRESS|none	IP address of router gateway to get to destination IP address.
config	yes|no	If enabled, appliance will transmit configuration changes to the specified IP address, to keep configurations in step.

Table 38: Share Parameters *(continued)*

Parameter	Value	Description
incident	yes|no	If enabled, appliance will transmit incident information to the specified IP address.
state	yes|no	If enabled, appliance will transmit connection state information to the specified address.
required	yes|no	If enabled, if the remote appliance is not available (which could be in a by-pass state), the local appliance will not be so rigorous in state checking.

Related Documentation

- DDoS Secure Appliance BGP Configuration on page 202
- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

show share

Syntax **show share <*IPADDRESS*|all>**

Description Displays the specified share configuration.

Sample Output

JS>show share all

```
set share 10.1.1.192 gateway none config yes incident yes state yes required no
set share 10.1.1.191 gateway none config yes incident yes state no required no
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove share

Syntax **remove share <*IPADDRESS*|all>**

Description Deletes the specified share. The <*IPADDRESS*> field should have a value that matches an existing defined share IP address. If the IP address used does not match any of the existing defined shares, the command is ignored.

It is also possible to delete all the defined shares. The command **remove share all** deletes all configured shares but prompts for confirmation before the command is accepted.

NOTE: When the value all is used with the remove share command the user is prompted if they are sure. This prompting can be turned off, which may be of use for scripted configurations.

Sample Output

```
JS>remove share all
Are you sure [yes/no]? yes

JS>show share all

set share 10.1.1.192 gateway none config yes incident yes state yes required no
set share 10.1.1.191 gateway none config yes incident yes state no required no

JS>remove share 10.1.1.191
JS>apply
JS>show share all
set share 10.1.1.192 gateway none config yes incident yes state yes required no
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set share

Syntax **set share <*IPADDRESS*> [gateway <*IPADDRESS*|none>] [config <yes|no>] [incident <yes|no>] [state <yes|no] [required <yes|no>]**

Description Defines the share. If all parameters are not present when defining a new share then any unspecified parameters are automatically set to **no**.

Sample Output

JS>show share all

```
set share 10.1.1.192 gateway none config yes incident yes state yes required no
```

JS>set share 10.1.1.191 config yes
JS>apply
JS>show share all

```
set share 10.1.1.192 gateway none config yes incident yes state yes required no
set share 10.1.1.191 gateway none config yes incident no state no required no
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

SNMP

The SNMP protocol can be used with DDoS Secure appliance to request data as well as send alerts. Thus, SNMP query related settings are also covered here. The same commands are used to manage settings that affect both SNMP alerts and queries. Table 39 on page 150 describes the SNMP parameters.

Table 39: SNMP Parameters

Parameter	Value	Description
trap	IPLIST|none	The IP address(es) to which SNMP traps are sent.
rocommunity	COMMUNITY	The community name required for read-only access to the SNMP variables.
trapcommunity	COMMUNITY	The community name used when sending SNMP traps.
syslocation	TEXT	A description of the location of the appliance unit.
syscontact	TEXT	Who to contact about the appliance unit.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show snmp

Syntax show snmp

Description Displays the current SNMP settings—the trap destination address, the read-only community string, the trap community string, the system location reference name, and the contact information for the system administrator.

Sample Output

JS>show snmp

```
set snmp trap 192.168.1.15 rocommunity public trapcommunity trapcom
 syslocation test-lab  syscontact
 support@DDoSsecureappliance-technology.com
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set snmp

Syntax **set snmp [trap <*IPLIST*|none>]**
[rocommunity <*COMMUNITY*>] [trapcommunity <*COMMUNITY*>]
[syslocation <*TEXT*>] [syscontact <*TEXT*>]

Description Adjusts the values of the SNMP trap address trap, the read-only community string rocommunity, the snmpcommunity string trapcommunity, the system location string syslocation, and the system admin contact syscontact.

Sample Output

JS>show snmp

```
set snmp trap 192.168.1.15 rocommunity public trapcommunity public
 syslocation test-lab  syscontact support@DDoSsecureappliance-technology.com
```

JS>set snmp syslocation “DDoS Secure appliance test lab”
JS>apply
JS>show snmp

```
set snmp trap 192.168.1.15 rocommunity public trapcommunity public
 syslocation “DDoS Secure appliance test lab” syscontact
 support@DDoSsecureappliance-technology.com
```

NOTE: Although **set snmp** allows the changing of both SNMP remote alerting and SNMP querying related settings, it does not change the security access settings to the appliance management interface. It is important that the **set access snmp** command also be used to ensure that trusted IP addresses have access to the appliance to be allowed to make SNMP queries.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Structured Syslog

The DDoS Secure appliance can be configured to send messages to a SEIM server in the following formats: STRM (also known as Log Event Extended Format or LEEF), Webtrends Enhanced Logging Format (WELF), or ArcSight Common Event Format (CEF). The remote SEIM server may require reconfiguration before it will accept DDoS Secure structured syslog messages. The SEIM server will receive the messages at the specified Facility and for Priorities greater than or equal to that configured. Table 40 on page 154 describes the structured syslog parameters.

Table 40: Structured Syslog Parameters

Parameter	Value	Description
ip	IPLIST|none	The IP address to which DDoS Secure will send structured syslog messages.
format	welf|leef|cef	The structured syslog format of the messages.
facility	SYSFACILITY	The syslog facility to which messages will be sent. If no previous facility has been defined and this parameter is not specified then the default daemon facility will be used.
priority	SYSPRIORITY	The syslog priority at or above appropriate messages will be sent. If no previous priority has been defined and this parameter is not specified then the default info priority will be used.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Syslog on page 156

show structured

Syntax show structured

Description Displays the current structured syslog configuration.

Sample Output

```
JS>show structured
set structured ip 192.168.1.99 format leef facility local0 priority info
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Syslog on page 156

set structured

Syntax **set structured [ip <*IPLIST*|none>] [facility <*SYSFACILITY*>] [priority <*SYSPRIORITY*>][format<welf|leef|arcsight>]**

Description Sets the structured syslog configuration, which is handled in the same was as ordinary syslog configuration.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Syslog on page 156

Syslog

The syslog protocol is based on the message logging system of the same name (see RFC3164—The BSD syslog protocol). A DDoS Secure appliance unit can be configured to send copies of messages that it records in its local log files to a remote syslog server. Table 41 on page 156 describes the syslog parameters.

Table 41: Syslog Parameters

Parameter	Value	Description
ip	IPLIST|none	The IP address(es) to which syslog messages will be sent.
facility	SYSFACILITY	The syslog facility to which messages will be sent. If no previous facility has been defined and this parameter is not specified then the default daemon facility will be used.
priority	SYSPRIORITY	The syslog priority at or above appropriate messages will be sent. If no previous priority has been defined and this parameter is not specified then the default info priority will be used.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show syslog

Syntax show syslog

Description Displays the current syslog configuration.

Sample Output

```
JS>show syslog
set syslog ip 192.168.1.15 facility local5 priority info
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set syslog

Syntax **set syslog [ip <*IPLIST*|none>] [facility <*SYSFACILITY*>] [priority <*SYSPRIORITY*>]**

Description Sets the syslog protocol. The DDoS Secure appliance has three syslog configuration settings, but the only one that must be configured for messages to be sent is the IP address of the remote syslog server.

The appliance will send syslog messages to the log file that are priority or higher.

Sample Output

```
JS>set syslog ip 192.168.0.10
JS>apply
JS>show syslog
set syslog ip 192.168.0.10 facility daemon priority info
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

TCP State Timeouts

It is possible to change the TCP State timeouts from their default values. Changing these values to low numbers can have a detrimental effect on the traffic flows and should only be done under the guidance of a DDoS Secure appliance engineer.

Table 42: Timeout Parameters

Parameter	Value	Default Value	Sends Keepalive	Sends RST on Session End
syn	STATETIMEOUT|default	10 seconds	–	–
s-a	STATETIMEOUT|default	7 seconds	–	Yes
s-s	STATETIMEOUT|default	10 seconds	–	–
ack	STATETIMEOUT|default	60 seconds	–	Yes
p-a	STATETIMEOUT|default	60 seconds	–	Yes
get	STATETIMEOUT|default	15 minutes	–	Yes
est	STATETIMEOUT|default	15 minutes	Yes	–
f1s	STATETIMEOUT|default	3 minutes	Yes	Yes
f2s	STATETIMEOUT|default	3 minutes	Yes	Yes

Table 42: Timeout Parameters *(continued)*

Parameter	Value	Default Value	Sends Keepalive	Sends RST on Session End
f3s	STATETIMEOUT|default	70 seconds	–	–
f-f	STATETIMEOUT|default	70 seconds	–	Yes
f1d	STATETIMEOUT|default	3 minutes	Yes	Yes
f2d	STATETIMEOUT|default	3 minutes	Yes	Yes
f3d	STATETIMEOUT|default	70 seconds		
cls	STATETIMEOUT|default	70 seconds	–	–
rst	STATETIMEOUT|default	30 seconds	–	–
r-c	STATETIMEOUT|default	30 seconds	–	–
unk	STATETIMEOUT|default	70 seconds	–	–
spf	STATETIMEOUT|default	10 seconds	–	–
sif	STATETIMEOUT|default	10 seconds	–	–
gets	STATETIMEOUT|default	2 minutes	–	–
ack80	STATETIMEOUT|default	20 seconds	–	Yes
url	STATETIMEOUT|default	10 seconds		
f2d80	STATETIMEOUT|default	20 seconds	–	Yes
swin	STATETIMEOUT|default	2 minutes	–	–

NOTE: Sends RST on session end is applicable only if, source and destination IP addresses of the session are both in defending mode.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show timeout

Syntax **show timeout [all|default]**

Description Displays the current state timeouts that do not have some of the default values, or all the default values.

Sample Output

```
JS>show timeout all
No timeout changes
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set timeout

Syntax **set timeout <PARAMETER> <VALUE> […]**

Description Sets the timeout value. The <*PARAMETER*> <*VALUE*> pair is taken from the timeout parameters.

Sample Output

```
JS>set timeout s-a 25
JS>apply
JS>show timeout all
set timeout s-a 25
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show decryptkeys

Syntax show decryptkeys<*all*|*IPADDRESS*>

Description Displays the decrypt key configuration. Each decrypt key definition can be configured as either default or specific. For default definitions, the ports and private key to be used for the decryption of SSL traffic to and from a protected IP address are specified. For a specific definition, a domain name and private key combination are applied in addition to the default configuration. An associated default configuration is required for a specific configuration for a protected IP address to exist.

Sample Output

JS>show decryptkeys all

```
nodle.pem
set decryptkeys default protected 192.168.1.189 ports 443 privatekey server.com.pem
set decryptkeys default protected 192.168.1.37 ports 443 privatekey f5-private.key
set decryptkeys specific protected 192.168.1.37 domain f5.com privatekey
 f5-private.key
set decryptkeys specific protected 192.168.1.37 domain testserver.com privatekey
 testserver.pem
set decryptkeys specific protected 192.168.1.37 domain server.com privatekey
 tserver.pem
set decryptkeys default protected 192.168.1.156 ports 443 privatekey test_pkey.pem
set decryptkeys default protected 192.168.1.157 ports 443 privatekey 157.pem
set decryptkeys default protected 192.168.21.125 ports 443 privatekey tserver.pem
```

The configurations associated with a single IP address can be shown by specifying the protected IP address as part of the command, as shown in the following example.

JS>show decryptkeys 192.168.1.37

```
set decryptkeys default protected 192.168.1.37 ports 443 privatekey f5-private.key
set decryptkeys specific protected 192.168.1.37 domain f5.com privatekey
 f5-private.key
set decryptkeys specific protected 192.168.1.37 domain testserver.com privatekey
 testserver.pem
set decryptkeys specific protected 192.168.1.37 domain server.com privatekey
 tserver.pem
```

JS>show decryptkeys stats

```
New Sessions Success                 :   592
Resumed Sessions Success             :  1241

Priv/Pub Key Mismatch                :     0
Failed RSA Decrypt                   :     0
No Private Key                       :     0
Failed Key Generation                :     0
Client Hello not seen                :     0
PFS Not Supported                    :    15
Key Exchange Not Supported           :     0
Unsupported Cipher                   :     0
Deflate Error                        :     0
Session setup not seen               :     0
Unknown compression                  :     0
Record Not Multiple of Block Size    :     0
```

```
Decryption Failed                        :     0
Session Resume Support Disabled          :     0
Session Resumed But Not Found            :     0
Unknown Message Type / Corrupt Header    :     0
Unrecognised Protocol Version            :     0
Invalid Record Size / Corrupt Header     :     0
Session setup not seen                   :     0
Not Configured for SSL Inspection        :     0
SSLv2 Inspection Not Supported           :     0
Failed Exchange Allocation               :     0
Failed Decrypt Allocation                :     0
Failed Deflate Allocation                :     0
Failed Deflater Allocation               :     0
Failed Record Allocation                 :     0
Failed Decoder Allocation                :     0
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set decryptkeys default

Syntax **set decryptkeys default protected <*IPADDRESS*> port <*PORTLIST*> privatekey <*PRIVATEKEY*>**

Description Set the ports and default private key for SSL inspection associated with the given protected IP address. The private key must be uploaded with the GUI beforehand and referenced by the filename.

Output Fields Table 43 on page 164 describes the decryptkeys default parameters.

Table 43: Decryptkeys Default Parameters

Parameter	Value	Description
protected	IPADDRESS	The protected IP address associated with this configuration.
ports	PORTLIST	The ports on which traffic to be decrypted is flowing.
privatekey	PRIVATEKEY	The filename of the private key used to decrypt the traffic.

Sample Output

```
JS>set decryptkeys default protected 192.168.1.40 ports 443 privatekey testserver.pem
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set decryptkeys specific

Syntax

set decryptkeys specific protected <*IPADDRESS*> domain <*DOMAIN*> privatekey <*PRIVATEKEY*>

Description

Adds a specific domain for SSL inspection in association with the protected IP address. The IP address must already have a default definition and the private key must be uploaded with the GUI beforehand, referenced by filename.

Output Fields

Table 44 on page 165 lists the decryptkeys specific parameters.

Table 44: Decryptkeys Specific Parameters

Parameter	Value	Description
protected	IPADDRESS	The protected IP address associated with this configuration.
domain	DOMAIN	The ports on which traffic to be decrypted is flowing.
privatekey	PRIVATEKEY	The filename of the private key used to decrypt the traffic.

Sample Output

```
JS>set decryptkeys specific protected 192.168.1.40 domain testitnow.com privatekey
privatekey.pem
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove decryptkeys

Syntax **remove decryptkeys <*all*|*IPADDRESS*>**

Description Removes the specified decrypt key configuration.

Sample Output

```
JS>remove decryptkeys 192.168.1.40
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Traffic Interception

The DDoS Secure appliance can generate pages that can be served back to the requesting client if the traffic would otherwise be dropped by a appliance filter. For further information on how to configure these, see subsequent chapters in this document

It is also possible to reverse the direction sense for specific VLANs where the notion of Internet and protected have to be reversed due to the network routing.

It is also possible to define whether some protocols are to be unwrapped to inspect the IP address packets contained within. IPv6 in IPv4, GRE tunnels, and GTP tunnels are supported. Table 45 on page 166 describes the traffic interception parameters.

Table 45: Traffic Interception Parameters

Parameter	Value	Description
enable	yes|no	Enables/disables response page generation.
respcode	CODE	HTTP response code to be generated.
http_ports	PORTLIST|none	HTTP response on these ports only.
https_ports	PORTLIST|none	HTTPS response on these ports only.
vlan	VLAN	Operates on this VLAN.
gtp	yes|no	Wraps IP packets (used by the mobile space) with a different outer set of IP headers and other information for routing traffic across mobile networks.
gre	yes|no	Wrasp IP packets with a different outer set of IP headers for routing traffic across networks.

Table 45: Traffic Interception Parameters *(continued)*

Parameter	Value	Description
ip6in4	yes|no	Wraps IPv6 packets with an outer IPv4 set of headers, so that the IPv6 traffic can be routed over an IPv4 network.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show wrapper

Syntax show wrapper <all|blocked|reverse|unwrap>

Description Displays the current wrapping configuration.

Sample Output

JS>show wrapper all

```
set wrapper blocked country enable yes respcode 200 http_ports 80
 https_ports none
set wrapper blocked ip enable yes respcode 200 http_ports 80 https_ports none
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set wrapper blocked

Syntax

```
set wrapper blocked country enable <yes|no>
http_ports <PORTLIST|none> https_ports <PORTLIST|none>
set wrapper blocked ip enable <yes|no>
http_ports <PORTLIST|none> https_ports <PORTLIST|none>
```

Description

Sets the wrapper blocked configuration. It is possible to set up a customized access denied page based on whether a country or IP address has been blacklisted. This is only done for the specified ports.

Sample Output

```
JS>set wrapper blocked country enable yes http_ports 80
JS>apply
JS>show wrapper all
set wrapper blocked country enable yes respcode 404 http_ports 80
 https_ports none
set wrapper unwrap gtp no gre yes ip6in4 yes
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set wrapper reverse

Syntax **set wrapper reverse vlan <*VLAN*>**

Description Sets the traffic that match the specific VLAN tag to be treated as if flowing in the opposite direction.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set wrapper unwrap

Syntax set wrapper unwrap <*gtp*|*gre*|*ip6in4*> <*yes*|*no*>

Description Defines the IP address protocols that are to be unwrapped and to inspect the IP address packets that are contained within.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

Usage

It is possible to define different table sizes for all the tracked information. The defined sizes are subjected to the amount of RAM, so the DDoS Secure appliance will reduces the values if they are too large.

Table 46 on page 171 describes the usage parameters and their format.

Table 46: Usage Parameters

Parameter	Value	Description
hwid	HARDWARE-ID	The hardware ID of the appliance.
bandwidth	BANDWIDTH	The purchased license count (in 1G units) to be shared across all DDoS Secure units.
protected	2|4|8|16|32|64|128|256|512|1K|2K|4K|8K|16K|32K|64K	The number of protected IP addresses.
portals	2|4|8|16|32|64|128|256	The number of protected portals.
filter	32|64|128|256|512|1K|2K|4K|8K|16K	The number of filter entries.
ratelimiters	2K|4K|8K|16K|32K|64K|128K|256K|512K|1M|2M|4M	The number of supported rate limiters.
tracked	128K|256K|512K|1M|2M|4M |8M|16M|32M	The number of tracked IP addresses.
macs	128|256|512|1K|2K|4K|8K|16K|32K	The number of MAC addresses.
tcps	128K|256K|512K|1M|2M|4M	The number of TCP sessions.
udps	128K|256K|512K| 1M|2M|4M	The number of UDP sessions.
icmps	2K|4K|8K|16K|32K|64K	The number of ICMP sessions.

Table 46: Usage Parameters *(continued)*

Parameter	Value	Description
others	2K|4K|8K|16K|32K|64K	The number of other IP address sessions.
frags	2K|4K|8K|16K|32K	The number of fragment sessions.
ftps	512|1K|2K|4K|8K|16K	The number of FTP sessions.
ssldecoders	512|1K|2K|4K|8K|16K	The number of decoders available for SSL inspection.
sslsessions	512|1K|2K|4K|8K|16K	The number of sessions cached for resumption during SSL Inspection.
sslhsbuffers	512|1K|2K|4K|8K|16K	The number of handshake buffers available for SSL inspection.
sslbbuffers	512|1K|2K|4K|8K|16K	The number of block buffers available for SSL inspection.
sslkx	512|1K|2K|4K|8K|16K	The number of key exchange buffers available for SSL inspection.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- **show usage on page 173**
- **set usage on page 174**

show usage

Syntax show usage

Description Displays the usage settings.

Sample Output

```
JS>show usage
set usage hwid 00:25:90:8E:55:0C bandwidth 10G protected 64K portals 256 filters
 4K ratelimiters 512K macs 16K tracked 32M tcps 4M udps 512K icmps 64K others 64K
 frags 16K ftps 8K httpparsers 8K ssldecoders 512K sslsessions 32K sslhsbuffers
 1K sslbbuffers 8K sslkx 32K
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Usage on page 171
- **set usage on page 174**

set usage

Syntax

```
JS>set usage
hwid Appliance hardware ID (if for another machine)
[bandwidth <BANDWIDTH>]
[protected <2|4|8|16|32|64|128|256|512|1K|2K|4K|8K|16K|32K|64K>]
[portals <2|4|8|16|32|64|128|256>]
[filters <32|64|128|256|512|1K|2K|4K|8K|16K>]
[ratelimiters <2K|4K|8K|16K|32K|64K|128K|256K|512K|1M|2M|4M>]
[tracked <128K|256K|512K|1M|2M|4M|8M|16M|32M>]
[macs <128|256|512|1K|2K|4K|8K|16K|32K>]
[tcps <128K|256K|512K|1M|2M|4M>]
[udps <128K|256K|512K|1M|2M|4M>]
[icmps <2K|4K|8K|16K|32K|64K>]
[others <2K|4K|8K|16K|32K|64K>]
[frags <2K|4K|8K|16K|32K>]
[ftps <512|1K|2K|4K|8K|16K>]
[httpparsers <1K|2K|4K|8K|16K|32K|64K|128K|256|512K|1M|2M>]
[ssldecoders <512|1K|2K|4K|8K|16K>]
[sslsessions <512|1K|2K|4K|8K|16K>]
[sslhsbuffers <512|1K|2K|4K|8K|16K>]
[sslbbuffers <512|1K|2K|4K|8K|16K>]
[sslkx <512|1K|2K|4K|8K|16K>]
```

Description Updates the usage tables.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Usage on page 171
- show usage on page 173

User Management

User accounts as determined by one of the following permissions. Users are only allowed to access their allocated portal information. Table 47 on page 174 describes the user access permission details.

Table 47: User Access Permissions

Parameter	Value
administrator	Has full access to change any configuration entry.
operator	Has full access to change any configuration entry other than user account configuration. Limited read-only access to user information.
guest	Has read-only access to configuration settings. Has no access to user information.

Table 47: User Access Permissions *(continued)*

Parameter	Value
sso	Can only change user information.

Table 48 on page 175 table describes the user parameters and their formats.

Table 48: User Account Parameters

Parameter	Value	Description
user	USERNAME	The username for this account.
password	PASSWORD	The user password.
perms	PERMS	The user access permissions.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8
- Access Control on page 18

show user

Syntax **show user <*USERNAME*|all>**

Description Displays the complete list of the configured user accounts. If the user using the command has administrator or sso permissions then the encrypted passwords are also shown along with the account name and permissions.

Sample Output

JS>show user all

```
set user user password $1$ehL5yai/$ewwyx0Oqx3VIdKXITvRUG. perms administrator
set user test password $1$wLh6yBh0$vmth1CmyrvQDg6ZKDTuqn. perms operator
```

Users with **operator** permissions will be shown the list of users without the passwords.

JS>show user all

```
set user user perms administrator
set user test perms operator
```

Alternatively, the details of a specific user can be shown if the username is specified instead of the parameter all.

This command is not available to guest accounts.

JS>show user test

```
set user test password $1$wLh6yBh0$vmth1CmyrvQDg6ZKDTuqn. perms operator
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

remove user

Syntax **remove user <*USERNAME*|all>**

Description Deletes a specific user. Only administrators can remove users, and they cannot delete themselves or change their own permission status.

This command can also be used to delete all current users. To do this the parameter value all is used instead of a user account name. Administrators can use remove user all but the command will not remove the administrator user account. When deleting all users the command will ask for confirmation.

NOTE: It is possible to disable the prompting, which can be useful for automated scripts.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set user

Syntax

set user<*USERNAME*> [password] <*PASSWORD*>
[perms <administrator|operator|guest|sso>]

Description

Creates a new user or modifies an existing one. When creating a new user the password must be specified. If the permissions are not specified then the permissions for the guest is assumed.

For an existing user account the **set user** command can be used to modify either the password or the permissions, or both.

When specifying the password either the encrypted form or a plain text password may be entered. An encrypted password, in the form of an MD5 hashed key, is recognized by the password starting with $1$.

NOTE: There is no echo suppression or masquerading of the input data when using the set user command, even when plain text password entry is in use.

CAUTION: Unlike the Web-based interface, there is no prompting for a repeat of the password entry, therefore extra care must be taken to avoid typing mistakes.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

CHAPTER 3

System Maintenance

This chapter describes the available system commands.

- system restart
- system restart_clear
- system shutdown
- system reboot
- system powerdown
- system factoryreset
- system config_reset
- system clear_custom
- system check
- system helpdesk

system restart

Syntax **system restart**

Description Restarts the DDoS Secure appliance software but does not restart the underlying operating system.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system restart_clear

Syntax

system restart_clear

Description

Restarts the DDoS Secure appliance software but does not restart the underlying operating system. All tables are cleared out, so the DDoS Secure appliance will need to re-learn everything.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system shutdown

Syntax system shutdown

Description Shuts down the DDoS Secure appliance engine only. The underlying operating system continues to run as does the GUI/CLI.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system reboot

Syntax **system reboot**

Description Reboots the DDoS Secure appliance.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system powerdown

Syntax **system powerdown**

Description Shuts down and powers off the DDoS Secure appliance.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system factoryreset

Syntax **system factoryreset**

Description Resets the DDoS Secure appliance configuration back to the factory default. This includes things such as IP addresses of the management interface and defined users.

NOTE: The DDoS Secure appliance will power off following the factory reset. Use **system config_reset** to prevent a power off.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system config_reset

Syntax **system config_reset**

Description Resets the DDoS Secure appliance configuration back to the factory default.

NOTE: This is same as **system factoryreset** but does not change the management IP and power off the appliance.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system clear_custom

Syntax **system clear_custom**

Description Removes any custom installed templates, certificates, or images.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system check

Syntax system check

Description Outputs a build and health check summary.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

system helpdesk

Syntax

```
system helpdesk
```

Description

Writes a copy of the HelpDesk file and the Hardware Diagnostics file to a formatted external USB drive.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

CHAPTER 4

Settings for Command-Line Environment

This chapter describes the settings for the CLI environment.

Terminal Configuration

Table 49 on page 191 describes the terminal configuration parameters and their formats.

Table 49: Terminal Configuration Parameters

Parameter	Value	Description
pause	*yes|no*	Enables or disables the automatic pause at the end of a screen of text. Disabling this feature can be useful in scripts to avoid the possibility of pauses which might interfere with the next line of the script. Default value is **yes**.
confirmations	*yes|no*	Enables or disables confirmations. Disabling confirmations will stop the prompts— **are you sure**, from appearing. This can be useful in scripts. Default value is **yes**.
lines	*LINES*	The number of vertical character lines the terminal is capable of displaying.
cols	*COLS*	The number of horizontal character columns the terminal is capable of displaying.
term	*TERMTYPE*	The terminal type. For example, vt220.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7

- Changing the Configuration Using the CLI on page 8

show terminal

Syntax show terminal

Description Displays the current terminal settings for this session.

Sample Output

```
JS>show terminal
set terminal pause yes confirmations yes lines 24 cols 80 term vt100
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

set terminal

Syntax

set terminal [pause <yes|no>] [confirmations <yes|no>] [lines <*LINES*>] [cols <*COLS*>] [term <*TERMTYPE*>]

NOTE: Only single parameter or value pair can be defined at once.

Description

Sets the terminal settings for the current CLI session. At the start of each new session the default values will be restored.

Sample Output

```
JS>set terminal pause yes
Terminal pause is now ON

JS>set terminal pause no
Terminal pause is now OFF
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

CHAPTER 5

Statistics and Informational Commands

This chapter describes statistics and informational commands.

- stats view
- show version
- ping

stats view

Syntax stats view

Description Displays the graphical output on the screen. Entering any key gives a list of all the available display options. The screen size and output format is based on terminal settings described in the chapter, *Settings for Command-Line Environment*.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

show version

Syntax show version

Description Displays the current software release along with other version details about the unit.

Sample Output

JS>sh version

```
DDoS Secure Code Version:      5.14.1-0
DDoS Secure Code Base:         CENTOS_6_3
DDoS Secure Build Date:        201305201820GMT
CD Base Image:                 5.14.1-0
Actual Memory Size:            31.3G
Actual Number of CPUs:         16
Serial No:                     A1RYMW1
Hardware ID:                   90:B1:1C:2A:A3:28
Platform:                      J-DDOS-SEC-AP2
Last Restart:                  Tue May 21 16:54:09 2013
Licensed Throughput:           10G
Memory To Use:                 31G
CPUs To Use:                   16
Protected IPs Supported:       64K
Tracked IPs Supported:         32M
Portals Supported:             256
Filters Supported:             4K
Rate Limiters Supported:       4K
MAC Entries Supported:         16K
TCP Entries Supported:         4M
UDP Entries Supported:         512K
ICMP Entries Supported:        64K
Other IP Entries Supported:    64K
Fragment Entries Supported:    32K
FTP Entries Supported:         8K
SSL Decoders Supported:        512K
SSL Sessions Supported:        512K
SSL Handshake Buffers:         1K
SSL Block Buffers:             2K
SSL Key Exchanges Supported:   512K
```

Table 50 on page 197 describes the information of each line.

Table 50: Show Version Parameters

Parameter	Description
DDoS Secure Code Version	The current version of the core DDoS Secure appliance software.
DDoS Secure Code Base	The underlying operating system.
DDoS Secure Build Date	When the build took place.
CD Base Image	The version of the CD used to re-image the unit.
Actual Memory Size	The available RAM.

Table 50: Show Version Parameters *(continued)*

Parameter	Description
Actual Number of CPUs	The number of CPU available.
Serial No	The serial number of the appliance.
Hardware ID	The ID key of the appliance.
Platform	The Juniper appliance model number.
Last Restart	The last time the DDoS Secure engine was restarted.
Licensed Throughput	This should match the size of the purchased license.
Memory To Use	Amount of memory the appliance is allowed to use.
CPUs To Use	Number of CPU the appliance is allowed to use.
Protected IP addresses Supported	The maximum number of protected IP addresses that can be tracked.
Tracked IP addresses Supported	Tracked IP addresses supported and the maximum number of Internet client IP addresses that can be tracked.
Portals Supported	The maximum number of portals supported.
Filters Supported	The maximum number of filters supported.
Rate Limiters Supported	The maximum number of rate-limiters supported.
MAC Entries Supported	The maximum number of MAC entries supported.
TCP Entries Supported	The maximum number of TCP sessions supported.
UDP Entries Supported	The maximum number of UDP sessions supported.
ICMP Entries Supported	The maximum number of ICMP sessions supported.
Other IP Entries Supported	The maximum number of other IP address sessions supported.
Fragment Entries Supported	The maximum number of fragment sessions supported.
FTP Entries Supported	The maximum number of FTP sessions supported.
SSL Decoders Supported	The number of decoders available for SSL inspection.
SSL Sessions Supported	The number of sessions cached for resumption during SSL Inspection.
SSL Handshake Buffers	The number of handshake buffers available for SSL inspection.

Table 50: Show Version Parameters *(continued)*

Parameter	Description
SSL Block Buffers	The number of block buffers available for SSL inspection.
SSL Key Exchanges Supported	The number of key exchange buffers available for SSL inspection.

It is possible to update the supported counts with the **set usage** command.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

ping

Syntax **ping <IPADDRESS>**

Description Provides the ability to ping an IP address that is routable over the management or DataShare interfaces for troubleshooting purposes.

NOTE: If Layer 2/3 or Layer 3 mode is configured, any IP addresses attached to or routed through the Internet or Protected interfaces will not respond to the ping command.

Sample Output

JS>ping 192.168.0.4

```
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
64 bytes from 192.168.0.4: icmp_seq=1 ttl=64 time=1.46 ms
64 bytes from 192.168.0.4: icmp_seq=2 ttl=64 time=0.411 ms
64 bytes from 192.168.0.4: icmp_seq=3 ttl=64 time=0.359 ms
64 bytes from 192.168.0.4: icmp_seq=4 ttl=64 time=0.401 ms
64 bytes from 192.168.0.4: icmp_seq=5 ttl=64 time=0.392 ms

--- 192.168.0.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.359/0.605/1.466/0.431 ms
JS>
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

CHAPTER 6

BGP Trigger Router Configuration

This chapter describes how a DDoS Secure appliance can act as a trigger router in a Remote Triggered Black Hole (RTBH) environment.

DDoS Secure BGP Trigger Router

The DDoS Secure appliance can act as a trigger router in a Remote Triggered Black Hole (RTBH) environment. It is then down to the BGP environment as to whether any IP address re-routed by the trigger router is either null routed, or re-routed through some other infrastructure.

The code was initially created for the appliance mitigation blade chassis—hence the CLI chassis syntax, where traffic can be re-routed through alternative blades. Something similar to the following lines are needed to get BGP working, where A.B.C.D is your DDoS Secure appliance management IP address, and W.X.Y.Z is the peering BGP router:

```
JS>set chassis blade ip A.B.C.D
JS>set chassis bgp ddos_secure A.B.C.D our_as 65099 neigh_ip
W.X.Y.Z neigh_as 65014 neigh_pass 123456
comm_as 65040 comm_no 99 lowertimer 300
```

```
JS>apply
```

This then generates a (quagga) configuration file on the appliance which is similar to the following (ip prefix-list not-ours deny are the local DDoS Secure appliance IP addresses).

NOTE: This is not the same as Configuring BGP Flow Spec, which does not use the Quagga process.

Related Documentation

- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99

DDoS Secure Appliance BGP Configuration

```
!
router bgp 65099
 bgp router-id A.B.C.D
 bgp log-neighbor-changes
 redistribute kernel route-map scrub-out
 redistribute static route-map scrub-out
 neighbor W.X.Y.Z remote-as 65014
 neighbor W.X.Y.Z password 123456
 neighbor W.X.Y.Z maximum-prefix 500
 neighbor W.X.Y.Z route-map scrub-out out
 neighbor W.X.Y.Z route-map scrub-in in
!
ip prefix-list not-ours seq 10 deny 1.1.1.128/30 le 32
ip prefix-list not-ours seq 20 deny 1.234.56.0/24 le 32
ip prefix-list not-ours seq 30 deny 169.254.0.0/16 le 32
ip prefix-list not-ours seq 40 deny 127.0.0.0/8 le 32
ip prefix-list not-ours seq 60 deny 192.168.0.0/24 le 32
ip prefix-list not-ours seq 70 deny 0.0.0.0/0
ip prefix-list not-ours seq 80 permit any
!
ip community-list 99 permit 65040:99
!
route-map scrub-out permit 10
 match ip address prefix-list not-ours
 set community 65040:99
!
route-map scrub-in deny 10
```

Related Documentation

- DDoS Secure BGP Trigger Router on page 201
- Network Configuration on page 99
- MAC Gateway Configuration on page 92

Peering Router Sample Configuration

```
!
router bgp 65014
bgp log-neighbor-changes
neighbor A.B.C.D remote-as 65099
neighbor A.B.C.D password 123456
 !
address-family ipv4
  redistribute connected route-map internal
  redistribute static route-map internal
  neighbor A.B.C.D activate
  neighbor A.B.C.D send-community
  neighbor A.B.C.D route-map scrubbing in
  neighbor A.B.C.D route-map scrubbout out
  no auto-summary
  no synchronization
exit-address-family
!
ip bgp-community new-format
ip community-list 99 permit 65040:99
```

```
!
ip prefix-list localdeny seq 5 permit 10.10.10.1/32
!
ip prefix-list scrubb seq 5 permit F.G.H.0/21 le 32
!
route-map scrubbing permit 10
match ip address prefix-list scrubb
match community 99 exact-match
set local-preference 200
set community no-advertise
set ip next-hop W.X.Y.Z
!
route-map scrubbout permit 10
match ip address prefix-list localdeny
```

Related Documentation

- DDoS Secure BGP Trigger Router on page 201
- Network Configuration on page 99
- MAC Gateway Configuration on page 92

Rerouting Trigger

These are based on the thresholds defined in the portal definition, and then applied to any IP address within that portal.

Table 51 on page 203 describes the portal definitions that will be actioned if BGP is enabled.

Table 51: Rerouting Trigger Parameters

Parameter	Description
rerouteminpkts	Packet rate has to remain below this threshold for at least lower timer seconds for the routing trigger to be removed.
reroutemaxpkts	Packet rate threshold for routing trigger to be invoked.
rerouteminspeed	Speed has to remain below this threshold for at least lower timer seconds for the routing trigger to be removed.
reroutemaxspeed	Speed threshold for routing trigger to be invoked.

Currently, only the protected IP address is inserted as a trigger route.

Related Documentation

- DDoS Secure BGP Trigger Router on page 201
- Network Configuration on page 99
- MAC Gateway Configuration on page 92

Force Specific Rerouting

Description Forces specific rerouting.

Sample Output

```
JS>set chassis reroute ip 1.2.3.4
JS>apply
```

Related Documentation

- DDoS Secure BGP Trigger Router on page 201
- Network Configuration on page 99
- MAC Gateway Configuration on page 92

CHAPTER 7

Understanding Blocked Country Response Configuration

Understanding BlackListed Traffic

Before configuring block country response, if a packet is detected coming from a country that has been blacklisted, the packet is simply dropped and recorded.

After configuring block country response, if a start of a new session packet comes from a country that is blacklisted and is a webpage request (to port 80, 443, or other optional ports), this is then redirected to an internal server that serves up a content page indicating that access from this country is blocked, potentially giving a reason why and some contact information. This allows the originator of the connection to request temporary access if they legitimately need it.

Related Documentation

- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99
- DDoS Secure BGP Trigger Router on page 201

Content Presentation Information

Filenaming Convention

There are a series of template files named blockedcountryXXXXYYYYZZZZ.tmpl or blockedcountryXXXXYYYYZZZZ.tmpl, where:

- XXXX optionally can be <DDoS Secure appliance portal name> where DDoS Secure appliance portal name is one of the optional user defined DDoS Secure appliance portals.
- YYYY optionally can be CCC where CCC is the 3 letter country code.
- ZZZZ optionally can be -www.domain.com.

The most specific match will be used with blockedcountryYYYY.tmpl overriding blockedcountryXXXX.tmpl.

Standard File Content

The content will be standard html (<html> ..... </html>) with replaceable keywords.

NOTE: Any references to external (to the page) information (for example: <img>, <frame>, href= and so on.) should be used with care, as they cannot be hosted on any of the protected websites as access to the references will also get (recursively) blocked.

Table 52 on page 206 describes keywords that can be recognized and replaced.

Table 52: File Content Parameters

Parameter	Description
%HOST%	Entry from the Host: Header.
%URL%	URL from the GET/POST/HEAD request. The host: header entry will be prefixed when appropriate.
%CCC%	Country name.
%IP%	Requesting IP address.
%TIME%	Current time of day (local time) in DAY MMM NNN HH:MM:SS YEAR format. For example: Wed Nov 30 21:49:08 2013).

Cache-control will be set to cache-control: no-cache, no-store in the response headers.

The page must be no more than 1000 bytes, so that it (along with the headers) can be sent back in a single packet.

The connection will be closed after serving the content.

If templates are not added, or are not matched, the following built-in template are used:

```
<html>
<h1>Access Administratively Blocked</h1>
<br>URL : '%URL%'
<br>Country : '%CCC%'
<br>Client IP address : '%IP%'
</html>
```

Related Documentation

- DDoS Secure Appliance Engine Configuration on page 207
- Network Configuration on page 99
- DDoS Secure BGP Trigger Router on page 201

Understanding Server Information

A simple webserver, running in a chroot, setuid environment on the DDoS Secure appliance. The blockedcountryXXXYYYYZZZZ.tmpl files will have the % keywords replaced at usage time.

The blockedcountryXXXYYYYZZZZ.tmpl files are updated through the DDoS Secure appliance GUI using the patch update mechanism. The patch update file (bc.upg) will (on a Linux system) need to be built with the following command:

```
echo 5.13 >webscreen- ; tar cvf bc.upg webscreen- blockedcountry*.tmpl
```

To delete a .tmpl file, repeat the line above, but without the file in question and re-install the bc.upg patch.

This server will handle both HTTP and HTTPS connections. For HTTPS connections, either a self-signed certificate or a CA signed certificate can be uploaded by including the file redirect.pem (which includes both the public and private key) in the bc.upg file.

Related Documentation

- DDoS Secure Appliance Engine Configuration on page 207

DDoS Secure Appliance Engine Configuration

The DDoS Secure appliance engine can be configured only through the CLI interface. The commands are:

- **show wrapper all**
- **show wrapper blocked**
- **remove wrapper blocked**
- **set wrapper blocked country enable <yes|no> respcode <resp code> http_ports <none|*PORT*> https_posts <none|*PORT*>**

Related Documentation

- Network Configuration on page 99
- DDoS Secure BGP Trigger Router on page 201

Testing the Country Codes for IP Addresses

It is possible to re-classify the country code for any IP address. The testing process is:

- Select and block a particular country. For example: pr (RFC1918 addresses).

  set block country –pr

- Reassign IP address through the CLI.

  set geoip ip code –pr ip 1.2.3.4

- Test with connections from the IP address 1.2.3.4 to get warning page.
- Add 1.2.3.4 to allow country block override list and verify that the normal page is reached.

  set block cignoreip 1.2.3.4

Reverse out configuration changes when finished.

NOTE: **If the DDoS Secure appliance Engine is in Logging mode, then this warning page will not get generated as all traffic is passed through anyway—even if a country is blocked.**

Related Documentation

- Network Configuration on page 99
- DDoS Secure BGP Trigger Router on page 201

Bypassing Country Block

You can configure Individual IP addresses, ranges, or subnets to override country blocking; so they are then allowed normal access, despite the traffic coming from a blocked country. This can be done through the GUI or CLI.

Related Documentation

- Network Configuration on page 99
- DDoS Secure BGP Trigger Router on page 201

APPENDIX A

Parameter Definitions

This appendix defines the syntax for the variable values that are used throughout this guide.

Variable Value Formats

Table 53 on page 209 describes the variable value formats.

Table 53: Variable Value Formats

Parameter Value	Example	Description
ACTION	discard	One of accept, discard, mark, redirect, ratelimit, sample, terminal, or sample-terminal.
ACTIONVALUE	100K	Appropriate value for *ACTION*. For example, *SPEED* and *COMMUMITY*.
ALERTINTERVAL	5	A positive value representing minutes.
ASLIST	1 - 3333, 3335 - 65535	A list of one or more comma separated *ASNUMBER* (max AS # 65535).
ASNUMBER	6523	An Autonomous System (BGP Routing) number.
AUTO-BACKLOG	auto-100	System rebooted.
AUTO-CONNECTIONS	auto-500	DDoS Secure engine prompts to restart.
AUTO-CONNRATE	auto-500	DDoS Secure engine prompts to shutdown.
AUTO-GETS	auto-500	Factory reset occurred.
BACKLOG	100	Software upgraded.
BANDWIDTH	2G	Number of software licenses (in 1G units) to be applied across a cluster of DDoS Secure devices.
BIAS	10	Configuration changed.

Table 53: Variable Value Formats *(continued)*

Parameter Value	Example	Description
COLS	80	Logging state started.
CONNECTIONS	500	Logging state with no TCP keepalives started.
CONNRATE	200	Defending state started.
COUNTRIES	all,!USA	A list of one or more *COUNTRYCODE* comma separated.
COUNTRYCODE	USA	Three letter country codes. A full list can be found in *Appendix C*. A prefix of ! means not this country. *all* means all countries.
DOMAIN	mydomain.com	A domain name.
DSCP	8	A Differentiated Services Code Point (DSCP).
DSCPLIST	3 - 4,8	A potentially mixed comma separated list of *DSCP* and *DSCPRANGE*. Spaces or line breaks must not be present within the list. Can be a single *DSCP* or *DSCPRANGE*.
DSCPRANGE	3 - 4	A range of inclusive *DSCP*s, separated by '-', specified in ascending order.
DISKNAME	/dev/sdb	Specific disk name.
DROPRATE	30	Rate above which traffic will get auto-black-listed.
EMAILADDRESS	support@ourdomain.com	Any valid e-mail address containing @ and a fully qualified domain.
MAILADDRESSES	user1@dom1.com, user2@dom2.com	One or more *EMAILADDRESS* that are comma separated.
EREGEX	^/index\.(asp|htm)$	Posix *EREGEX*.
FCMODE	none	The flow control mode of the interface. Valid values are none, tx_only, rx_only, full, and auto. *FCMODE* auto is only supported if *LINKMODE* is set to auto.
FILTERNAME	Inweb	Can be any printable character other than a space. Maximum length is 15 characters.
FILTERS	10	The number (of limited) filters to allocate to this portal.
FLOWFLUSH	1	A positive value between 1 and 60 inclusive (in minutes).
FREQUENCY	d	One of h(our), d(ay) or w(eek).

Table 53: Variable Value Formats *(continued)*

Parameter Value	Example	Description
GETS	200	A single non-negative number, or *U*.
GROUPINGID	1	An integer between 1 and 254 inclusive.
HAMODE	active-standby	Valid modes are *standalone*, *active-standby*, *active-standby-fs*, and *load-share-mc*.
HARDWARE-ID	00:01:02:03:04:05	Six hexadecimal values separated by colons. Case insensitive.
HEADER	X-Forwarded-For:	Must include trailing : and this is case insensitive.
ICMPCODE	8	An ICMP code number in the range 0 to 255.
ICMPCODELIST	3 - 4,8	A potentially mixed comma separated list of *ICMPCODE* and *ICMPCODERANGE*. Spaces or line breaks must not be present within the list. Can be a single *ICMPCODE* or *ICMPCODERANGE*.
ICMPCODERANGE	3 - 4	A range of inclusive *ICMPTYPE*s, separated by '-', specified in ascending order.
ICMPTYPE	8	An ICMP type number in the range 0 to 255. 18 is the largest currently defined type.
ICMPTYPELIST	3 - 4,8	A potentially mixed comma separated list of *ICMPTYPE* and *ICMPTYPERANGE*. Spaces or line breaks must not be present within the list. Can be a single *ICMPTYPE* or *ICMPTYPERANGE*.
ICMPTYPERANGE	3 - 4	A range of inclusive *ICMPTYPE*s, separated by '-', specified in ascending order.
ICMP6TYPE	128	An ICMP6 type number in the range 0 to 255. 18 is the largest currently defined type.
ICMP6TYPELIST	128 - 129,131	A potentially mixed comma separated list of *ICMP6TYPE* and *ICMP6TYPERANGE*. Spaces or line breaks must not be present within the list. Can be a single *ICMP6TYPE* or *ICMP6TYPERANGE*.
ICMP6TYPERANGE	128 - 129	A range of inclusive *ICMP6TYPE*s, separated by '-', specified in ascending order.
IPADDRESS	192.168.1.1	A single host entry (can be IPv6).
IPBLOCK	192.168.0.3-192.168.0.9	A contiguous block of IP addresses (can be IPv6).
IPLIST	192.168.1.1,192.158.0.3	One or more comma separated *IPADDRESS* entries.

Table 53: Variable Value Formats *(continued)*

Parameter Value	Example	Description
IPMULTI	225.0.0.1	A multi-cast IP address.
IPNETWORK	192.168.2.0/24	A network entry in network/bits format, it uses a bit count mask entry (can be IPv6).
IPNETWORK	192.168.3.0/255.255.255.0	A network entry in network/mask format, uses a dotted decimal mask entry.
IPRANGE	10.1.1.1,10.1.2.0/24 10.1.3.0/255.255.255.0, 192.168.0.3-192.168.0.9	A potentially mixed comma separated list of *IPADDRESS*, *IPNETWORK*, and *IPBLOCK*. Spaces or line breaks must not be present within the list. Can consist of a single *IPADDRESS*, *IPNETWORK*, and *IPBLOCK* (can be IPv6).
LENGTH	100	A packet length, including the IP headers.
LENGTHLIST	100 - 200,300	A potentially mixed comma separated list of *LENGTH* and *LENGTHRANGE*. Spaces or line breaks must not be present within the list. Can be a single *LENGTH* or *LENGTHRANGE*.
LENGTHRANGE	100 - 200	A range of inclusive *LENGTH*, separated by '-', specified in ascending order.
LICENSE-KEY	78c683db-2de85144-86424180-d868a089-4c329901-205a4986-075f8d0c	62 characters long and case sensitive (without newlines).
LIFETIME	60	A positive value between 30 and 6000 inclusive (in minutes).
LIMIT	15	Limit above which traffic will get auto-black-listed.
LINES	24	A valid positive number. Default value is 24.
LINKMODE	100full	The link mode of the interface. Valid values are *10half*, *10full*, *100half*, *100full*, *1000full*, *10000full* and *auto*. Not all values may be supported depending on the Webscreen model.
MAC	00:02:04:06:08:10	A single 6-byte Ethernet MAC entry. This entry may be followed parameters describing the VLAN or MPLS labels associated with this MAC address as follows: • v VLAN • q QINQ • u Unicast MPLS label • m Multicast MPLS label
MODE	defensive	Valid modes are *defending*, *defending-nostatelearn*, *logging*, *logging-nokeepalives*, *logging-tap*, *bypass-software*, and *bypass-fs-hardware*.

Table 53: Variable Value Formats *(continued)*

Parameter Value	Example	Description
MODEIP	defensive	Valid modes are *defending*, *logging*, and *notreported*.
MODEPORTAL	defensive	Valid modes are defending and logging.
MTU_SIZE	1500	IP Packet length with 16 bytes for vlans/mpls.
NETMASK	255.255.255.0	A network mask in dotted decimal mask entry.
PASSWORD	mypassword	Must contain printable characters and have a maximum length of 35 characters when not encrypted.
PERMS	administrator	One of administrator, sso, operator, or guest.
PKTS	3.7K	Packet rate for the appropriate threshold.
PORT	22	A port number in the range 1 to 65535.
PORTALNAME	portal123	Starts with a alpha character, contains alpha-numeric characters, “.”, “_” and “-“. Maximum length is 15 characters.
PORTLIST	22, 35 - 40	A potentially mixed comma separated list of *PORT* and *PORTRANGE*. Spaces or line breaks must not be present within the list. Can be a single *PORT* or *PORTRANGE*.
PORTRANGE	35 - 40	A range of inclusive *PORT*s, separated by "-", specified in ascending order.
PRIORITY	1	Priority weighting for failover systems to determine if a system is a natural active. Valid values are -127 to 127.
PROTECTED	10	The number (of limited) protected IPs to allocate to this portal.
PROTECTEDNAME	webserver1	Starts with an alpha-numeric character, contains alpha-numeric characters, “_”, “-“, and “.”. Maximum length is 31 characters.
PROTOCOL	47	A protocol number in the range 1 to 255. NOTE: Protocols 1 (ICMP), 6 (TCP), and 17 (UDP) are handled separately and ignored if specified here.
PROTOCOLLIST	22, 35 - 40	A potentially mixed comma separated list of *PROTOCOL* and *PROTOCOLRANGE*. Spaces or line breaks must not be present within the list. Can be a single *PROTOCOL* or *PROTOCOLRANGE*.
PROTOCOLRANGE	50 - 51	A range of inclusive *PROTOCOL*s, separated by ‘-‘, specified in ascending order.

Table 53: Variable Value Formats *(continued)*

Parameter Value	Example	Description
RATE	100	An integer value between 0 and 65535 packets per second.
REGEX	^/index.asp$	Posix REGEX. Use end and start locators to prevent false matches.
RESPCODE	503	3 digit response code.
SECRET	serverPassword	Must contain printable characters and has a maximum length of 128 characters.
SERVERNAME	webserver1	Starts with an alpha-numeric character, contains alpha-numeric characters, "_", "-", and ".". Maximum length is 31 characters.
SPEED	10M	Speed in bits per second (bps). The numeric value can be suffixed with K, M, or G as appropriate. All speeds are rounded down to a multiple of 8 bps.
STATETIMEOUT	30	A value between 2 and 3600 seconds.
STRING	/index.asp	Any printable characters.
SYSFACILITY	local1	One of *auth*, *cron*, *daemon*, *kern*, *lpr*, *mail*, *new*, *user*, *uucp*, *syslog*, *local0*, *local1*, *local2*, *local3*, *local4*, *local5*, *local6*, or *local7*. The receiving Syslog server must be configured to accept and redirect the Syslog information based on *SYSFACILITY* and *SYSPRIORITY*.
SYSPRIORITY	info	One of *alert*, *crit*, *debug*, *emerg*, *err*, *info*, *notice*, or *warning*.
TEMPLATEP	1000	A positive value between 1 and 1000 inclusive.
TEMPLATEM	60	A positive value between 1 and 3600 inclusive (in minutes).
TERMTYPE	vt220	The terminal type. Default is vt100.
TEXT	"some text contained within quotes"	Any printable character excluding ". The text must be enclosed in quotes if there are any spaces.
THRESHOLD	10	Erroneous packets per second.
THRESHOLDTIME	60	Time in seconds before something happens.
TIMEOUT	5	A positive value between 1 and 60 inclusive (in minutes).

Table 53: Variable Value Formats *(continued)*

Parameter Value	Example	Description
TIMESTRING	“24-jan-03 16:00:00”	Can be one of the following formats: • yyyy-mm-ddThh:mm:ss (preferred) • dd mmm yyyy hh:mm:ss • dd-mmm-yy hh:mm:ss • mmm dd hh:mm:ss yyyy
TIMEZONE	Europe/London	The full list of available timezones can be found by using the **show timezones** command.
TPROTOCOL	lcp	The notional protocol in use.
TSERVICE	Webscreen	Request to use particular service.
URL	http://f.t.com/file.txt	URL containing IP address information.
USERNAME	user123	Starts with a lower alpha character, contains lower alpha-numeric characters, “_”, and “-“. Maximum length is 20 characters.
VALUE	100	An integer value between 0 and 65535.
VLANSDEF	v1024,m1234	A potentially mixed, comma separated list of Vlan definitions or MPLS labels.

Table 54 on page 215 lists the fixed value formats.

Table 54: Fixed Value Formats

Parameter Values	Specific Area	Description
10000full	Interface	To be forced to 10G full duplex.
1000full	Interface	To be forced to 1G full duplex.
100full	Interface	To be forced to 100M full duplex.
100half	Interface	To be forced to 100M half duplex.
10full	Interface	To be forced to 10M full duplex.
10half	Interface	To be forced to 10M half duplex.
active-standby	Appliance	Webscreen is to be run as part of an Active Standby configuration.
active-standby-fs	Appliance	Webscreen is to be run as part of an Active Standby configuration with fail-safe card enabled.

Table 54: Fixed Value Formats *(continued)*

Parameter Values	Specific Area	Description
administrator	User	User role that has full administrative rights.
alert	Syslog	Logging Level.
all		All valid entities matched.
auth	Syslog	Logging Facility.
auto	Interface	Auto negotiate configuration.
autodetected		Items that have been auto-detected by the Webscreen, but not configured.
bl	GeoIP, URL, DNS	Item it to be black-listed.
bl+	DNS	Item is to be black-listed, even if logging.
broadcast		The settings for all servers responding to broadcast MAC address.
bypass-fs-hardware	Appliance	Pass all traffic straight through the fail-safe card.
bypass-software	Appliance	Pass all the traffic straight through using software.
crit	Syslog	Logging Level.
cron	Syslog	Logging Facility.
daemon	Syslog	Logging Facility.
debug	Syslog	Logging Level.
default	Protected	The default server settings, used for unspecified server fields or by autodetected servers.
default		The default settings.
defending	Appliance, Portal, Protected	Enabled for defending.
defending-nostatelearn	Appliance	Diagnostic mode where state learning is disabled.
emerg	Syslog	Logging Level.
err	Syslog	Logging Level.
full	Interface	Force full flow control.
guest	User	User role that has only read-only access.

Table 54: Fixed Value Formats *(continued)*

Parameter Values	Specific Area	Description
indeterminate	Protected	The settings for all servers detected by Webscreen after filling its internal server table, or for traffic to an IP address that has not yet been confirmed as a genuine server.
info	Syslog	Logging Level.
intercept	Protected	Server used to generate response failure pages.
kern	Syslog	Logging Facility.
load-share-mc	Appliance	Appliance is to be run in a load sharing environment using multi-cast MAC addresses.
local0	Syslog	Logging Facility.
local1	Syslog	Logging Facility.
local2	Syslog	Logging Facility.
local3	Syslog	Logging Facility.
local4	Syslog	Logging Facility.
local5	Syslog	Logging Facility.
local6	Syslog	Logging Facility.
local7	Syslog	Logging Facility.
logging	Appliance, Portal, Protected	Enabled for logging only (keepalives generated).
logging-nokeepalive	Appliance	Enabled for logging only.
logging-tap	Appliance	Enabled for TAP mode.
lpr	Syslog	Logging Facility.
mail	Syslog	Logging Facility.
multicast		The settings for all servers responding to multicast MAC addresses.
news	Syslog	Logging Facility.
no		Disable this item.
none		Effectively disable this item.

Table 54: Fixed Value Formats *(continued)*

Parameter Values	Specific Area	Description
notice	Syslog	Logging Level.
notreported	Protected	Nothing is reported for traffic to this IP.
operator	User	User role that has full rights, apart from configuring users.
rx_only	Interfaces	Force flow control to only receive.
sso	User	User role that can only configure users.
standalone	Appliance	Webscreen is not part of an Active-Standby relationship.
standalone-nofs	Appliance	Appliance is not part of an Active-Standby relationship, and the fail-safe card is to be disabled.
tx_only	Interfaces	Force flow control to only transmit.
user	Syslog	Logging Facility.
uucp	Syslog	Logging Facility.
warning	Syslog	Logging Level.
wl	GeoIP, URL, DNS	Whitelist the item.
yes		Enable this item.
U		Unrestricted.

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

APPENDIX B

Structure Syslog Details

Structure Syslog Description

DDoS Secure supports three different structured syslog formats: the legacy WebTrends format (WELF), STRM format (LEEF), and ArcSight format (CEF). The format is selectable under the structured syslog option of the GUI or the CLI.

Each message format consists of an Event ID field and a number of different parameters. The message parameters for the different formats are described from Table 56 on page 221 through Table 60 on page 235 based on the type of event being reported.

Table 55 on page 219 describes the types of structured syslog messages.

Table 55: Structured Syslog Message Types

Message Type	Range	Description
Standard Administration Messages	1001 - 1xxx	• Sent out as events happen. • Includes Health Check messages, sent out at 5-minute intervals, which contain information about licensing usage.
Appliance Defense States	2001 - 2xxx	Reflects the status of the right pane as it turns red.

Table 55: Structured Syslog Message Types *(continued)*

Message Type	Range	Description
Incidents	3001 - 3xxx	a. An Incident Active message is sent out when an attack exceeds **threshold alert** and that has been ongoing for longer than the value of **incidents threshold**: 1. From GUI -> **Incident Alert Threshold** 2. From CLI -> **show threshold alert** 3. From CLI -> **show incidents** b. An Incident Active Update message is sent out periodically while the attack is active. The frequency is determined by **incidents logrefresh**. 1. From CLI -> **show incidents** c. An Incident Active Complete message is sent out when the incident is either idle or closed down because its lifetime has expired. If an attack is still active after the incident is closed down and the conditions in Step i are met, a new incident with a new incident ID is created. d. An Incident Detail message is sent only if it is configured with the CLI command **set debugging incidentdetail yes** (the default is **no**). Otherwise, only summary Incident messages are sent. e. An Incident Detail message includes the top 10 IPs, as well as a **remaining** entry where the IP address is 0.0.0.0.
Worst Offenders	4001 - 4xxx	a. A Worst Offender Start message is created whenever an IP address is marked as being a Worst Offender and exceeds **threshold offenders**. 1. From CLI -> **show threshold offenders** b. A Worst Offender Complete message is sent whenever an IP address is removed from the Worst Offender list. c. A Worst Offenders message is sent only if it is configured with the CLI command **set debugging worstoffenders yes** (the default).
Temporary Black List	5001 - 5xxx	Thresholds are configurable for transitioning an IP address from Worst Offenders (occasional packets dropped) to Temporary Black List (all packets dropped). 1. From GUI -> Configure DDoS Secure 2. From CLI -> **show appliance** a. A Temporary Black List Start message is created whenever an IP address is marked as being a Temporary Black List IP. These are the IP addresses from which or to which DDoS Secure does not allow traffic. b. A Temporary Black List Update message is sent out periodically when the attack is active. The frequency is determined by **incidents logrefresh**. c. A Temporary Black List Complete message is sent whenever an IP address is removed from the Temporary Black List list. d. A Temporary Black List message is sent only if it is configured with the CLI command **set debugging autoblacklist yes** (the default).
Permanent White-List/Black-List	6001 - 6xxx	• These messages are sent out every time there is a configuration file change that affects the permanently defined white-list or black-list definitions. • These messages are sent out every hour. • Information for a definition is concatenated (comma separated) subject to a maximum of 1,000 characters per record. • Information is continued in the next record.

Event Types

Table 56 on page 221 through Table 60 on page 235 describe event types.

Table 56: Basic Events

Event ID	Event Name	Description
1001	User Login	User logs in to the system. Reports valid and failed login attempts.
1002	User Logout	User logs out of the system.
1003	Create User	User created on the system.
1004	Modify User	User updated on the system.
1005	Delete User	User deleted from the system.
1006	Power Off	System powered off.
1007	Reboot	System rebooted.
1008	DDoS Secure Engine Start	DDoS Secure engine directed to start.
1009	DDoS Secure Engine Restart	DDoS Secure engine directed to restart.
1010	DDoS Secure Engine Shutdown	DDoS Secure engine directed to shut down.
1011	Factory Reset	Factory reset occurred.
1012	Software Upgrade	Software upgraded.
1013	Configuration Changed	Configuration changed.
1014	Logging State	Logging state started.
1015	Logging State No Keep Alives	Logging state with no TCP keepalives started.
1016	Defending State	Defending state started.
1017	Defending State No Keep Alives	Defending state with no TCP keepalives started.
1018	IPMI	IPMI messages.
1019	Cover Intrusion Detected	Cover intrusion detected.
1020	Power Supply Failure	Power supply failure.
1021	Disk Write Error	Disk write error.
1022	Disk SMART Info	Disk SMART info received.

Table 56: Basic Events *(continued)*

Event ID	Event Name	Description
1023	Interface Restart	Internet or Protected interface restarted.
1024	HA State Standalone	High availability standalone state entered.
1025	HA State Active Standby	High availability active state entered.
1026	HA State Load Share	High availability load share state entered.
1027	HA State Activity Standby FS	High availability active standby with fail-safe state entered.
1028	Administrative Information	Administrative messages.
1029	SSL	SSL messages.
1030	Configuration	Configuration changes and updates.
1031	Dropped	Messages dropped because of heavy processing load.
1032	Debug	Debug information.
1033	Watchdog	Watchdog messages.
1034	Health Check	Health Check messages, including licensing usage information.

Table 57: Additional Status Events

Event ID	Event Name	Description
2001	Output Error – Protected	The DDoS Secure appliance is having trouble transmitting packets on the Protected interface. This might be caused by a downstream link being saturated or a duplex speed mismatch.
2002	Output Error – Internet	The DDoS Secure appliance is having trouble transmitting packets on the Internet interface. This might be caused by a downstream link being saturated or a duplex speed mismatch.
2003	Output Error – Management	The DDoS Secure appliance is having trouble transmitting packets on the Management interface. This might be caused by a downstream link being saturated or a duplex speed mismatch.
2004	New Configuration	This is in response to the configuration being updated, potentially by a remote Webscreen.
2005	Not Licensed	The DDoS Secure appliance is not authorized for use.
2006	MAC Table Full	The appliance has run out of internal table space for MAC addresses. The oldest (by use) entry has been dropped.

Table 57: Additional Status Events *(continued)*

Event ID	Event Name	Description
2007	Protected IP Table Full	The appliance has run out of internal table space for protected IP addresses. This usually indicates that your Internet and protected cable connections are swapped. If not, then your appliance is trying to protect too many protected IPs and the network topology needs to be reviewed, or a feature upgrade should be purchased (if available).
2008	INCIDENT Table Full	The appliance has run out of internal table space for active Incidents. The oldest (by use) entry has been dropped.
2009	TCP Table Full	The appliance has used all the internal table space for TCP connections. The entries that are not required are removed to create space for the next TCP connection. This should normally happen only when defending against a large-scale attack.
2010	UDP Table Full	The appliance has used up all the internal table space for UDP sessions. The entries that are not required are removed to create space for the next UDP session. This should normally happen only when defending against a large-scale attack.
2011	ICMP Table Full	The appliance has run out of internal table space for ICMP sessions. This table size is deliberately restricted. The oldest (by use) entry has been dropped. This should normally happen only when defending against a large-scale attack.
2012	Other-IP Table Full	The appliance has used up all the internal table space for IP protocol sessions. The entries that are not required are removed to create space for the next IP protocol session. This should normally happen only when defending against a large-scale attack.
2013	FRAGMENT Table Full	The appliance has run out of internal table space for handling fragments. This table size is deliberately restricted. The oldest (by use) entry has been dropped.
2014	FTP Table Full	The appliance has used up all the internal table space for tracking FTP connections. The entries that are not required are removed to create space for the next FTP connection. This should normally happen only when defending against a large-scale attack.
2015	Black-Listed IP Table Full	The appliance has used up all the internal space for tracking IP addresses that are being temporarily black-listed. Any inactive black-listed IP address will be removed from the list.

Table 57: Additional Status Events *(continued)*

Event ID	Event Name	Description
2016	Network Short Circuit	The DDoS Secure appliance has detected the same source MAC address in use on both the I-I/F and P-I/F interfaces. Bypass packets are not passed through the appliance when it is in defensive mode. This means that there is either an alternative data path around the appliance, or a topology change has placed a previously determined MAC address on the opposite side of the appliance. In the event of a topology change the cached entry can be modified by configuring the MAC address as either an Internet or a protected gateway; or if not configured, the MAC will be allowed to change sides automatically after 5 seconds.
2017	Internet-I/F N/C	The Internet interface is not physically connected. This occurs when the appliance is running as STANDBY in a VMware environment.
2018	Protected-I/F N/C	The Protected interface is not physically connected.
2019	Management-I/F N/C	The Management interface is not physically connected.
2020	Upgrading	The DDoS Secure appliance is undergoing a software update.
2021	Rate Limit Table Full	The appliance has run out of internal table space for handling rate limiters. You cannot create any new rate limiters until the existing ones expire.
2022	Routing Loop	The DDoS Secure appliance has detected that a packet that has just been passed through the appliance is now returning back through the appliance. This usually indicates that two routers, one on either side of the appliance, have incorrectly determined that traffic needs to be redirected through the opposite router to get to a specific IP address.
2023	Forced Inactive	The appliance has detected a network short circuit before the system is licensed. Consequently, no more traffic will be passed through until the bypass situation is sorted out and the appliance is restarted.
2024	State Learning	For the first 5-minute after a reboot or a network cable being plugged in, the DDoS Secure appliance bypasses State Table rigorous checking, so that existing connections that are active when the appliance becomes active are not blocked. Override this 5-minute window by setting the appliance to Defending-NoStateLearn mode.
2025	Support Expired	The DDoS Secure appliance support license has expired.
2026	Sever Loading	The appliance has detected that some packets have been dropped as a result of heavy loading. Logging activity has been substantially reduced to minimize the further dropping of any packets.

Table 57: Additional Status Events *(continued)*

Event ID	Event Name	Description
2027	MAC Misconfigured	A MAC address has been defined as an Internet or Protected address type, but the address has also been detected on the opposite side of the DDoS Secure appliance. Correct this situation.
2028	Interface Speed Mismatch	On fail-safe systems, the interface speeds on the fail-safe card are defined, or detected to be different, which will cause an issue if the card becomes fail-safe.
2029	Internet Sub-Link Down	One of the links on the Internet interface is not physically connected.
2030	Protected Sub-Link Down	One of the links on the Protected interface is not physically connected.
2031	DataShare-I/F N/C	The Data Share interface is not physically connected, and has an IP address configured.
2032	Disk Failure	One of the disks has failed a SMART test and should be replaced as soon as possible.
2033	PSU Failure	The system BIOS is reporting that one of the redundant power supplies is not working or not powered up. This situation needs to be rectified as soon as possible to prevent the appliance from losing power should the working PSU fail.
2034	Fan Failure	The system BIOS is reporting that there has been a fan failure, or that the appliance is running in a hot environment. This needs to be repaired as a soon as possible to prevent hardware component failure.
2035	Config Transfer Failed	The DDoS Secure appliance was unable to transmit the configuration file changes to a partner.
2036	Missing Partner	A State Synchronization partner defined as required is not available. The DDoS Secure appliance is running in a degraded state, where all DDoS activity will not be detected and protected against.
2037	BGP Misconfigured	The DDoS Secure appliance has detected a BGP session but the server is excluded by the DDoS Secure appliance portal network list.
2038	Missing State Packets	The DDoS Secure appliance has detected that some state synchronization packets were not received.

Table 58: Incident Events

Event ID	Event Name	Description
3001	Bandwidth	Bandwidth rate exceeded for MAC address, portal, or filter.

Table 58: Incident Events *(continued)*

Event ID	Event Name	Description
3002	Packet Rate	Packet rate exceeded for MAC address, portal, or filter. The appliance has detected high rates of small packets.
3003	Blocked Protocol – Black-Listed	This IP address has been black-listed, because it is has been defined as part of a black-listed network.
3004	Blocked Protocol – Icmp Type	No filters match for this ICMP packet.
3005	Blocked Protocol – Port	No filters match for this destination port.
3006	Blocked Protocol – Other Proto	No filters match for this protocol type.
3007	Not Passed Thru – Runt Packet	Undersized packet has been dropped.
3008	Unknown Session – Icmp Response	ICMP response packet has no matching ICMP request in the state table.
3009	Unknown Session – Icmp Diag Response	ICMP diagnostic response packet does not match a state table entry for the respective IP protocol.
3010	Unknown Session – No State	TCP packet has no state table entry and is not a SYN packet.
3011	Unknown Session – Invalid State	TCP packet has a state table entry, but packet is out of state.
3012	TCP Attack – RST	RST packet has invalid sequence number.
3013	IP Attack – Land	Source and destination IP addresses are equal.
3014	TCP Attack – Syn-Ack Timeout	The client IP did not complete the TCP connection.
3015	Block Protocol – Black-Listed Country	Traffic to or from a country has been blocked, because the country is black-listed.
3016	TCP Attack – Syn Flood	The protected IP is receiving SYN packets at a rate higher than it is configured for or can handle.
3017	TCP Attack – Connection Flood	The protected IP has reached its concurrent connection configured limit.
3018	TCP Attack – Table Full	Internal state table for TCP connections is being CHARM protected.
3019	Bad TCP Packet – Fast Repeat Ack	Identical packets containing ACKs are being repeated at a rate of greater than 10 per second.
3020	TCP Attack – HTTP Flood	The protected IP has reached its concurrent GET/HEAD configured limit.
3021	UDP Attack – Table Full	Internal state table for UDP information is full.

Table 58: Incident Events *(continued)*

Event ID	Event Name	Description
3022	Not Passed Thru – Pause Frame	Ethernet pause frame has been dropped.
3023	TCP Attack – HTTP Timeout	The protected IP did not respond to a GET/HEAD request in a timely manner.
3024	ICMP Attack – Repeats	ICMP packets being repeated at a rate of more than 40 per second.
3025	ICMP Attack – Table Full	Internal state table for ICMP is being CHARM protected.
3026	Not Passed Thru – State Sync	State Synchronization packets are being processed but not passed through.
3027	Other-IP Attack – Table Full	Internal state table for Other Ips is being CHARM protected.
3028	Not Passed Thru – State Sync Sent	State Synchronization packets are being processed but not passed through.
3029	Fragment Attack – Ping of Death	Assembled packet is longer than 65,535 bytes.
3030	Fragment Attack – Header Overlay	Fragment start overlays protocol header.
3031	Fragment Attack – Table Full	Internal state table for fragments is being CHARM protected.
3032	Fragment Attack – Small Size	Initial TCP fragment is smaller than header.
3033	Fragment Attack – No Fragments allowed	No fragmented packets are allowed to or from this protected IP.
3034	Bad IP Packet – Invalid Source Address	IP packet has invalid source address.
3035	Bad IP Packet – Broken Header	IP header malformed – RFC non-compliant.
3036	Bad IP Packet – Invalid Option	IP packet has invalid option field or field length.
3037	Bad IP Packet – Size Mismatch	IP packet has invalid field length.
3038	Blocked Protocol – Temp Black-Listed	This IP address has been temporarily black-listed because of its aggressive behavior.
3039	Bad TCP Packet – Flags	Invalid TCP flags combinations.
3040	Bad TCP Packet – Malformed	Format of TCP header invalid.
3041	Bad TCP Packet – Option	Invalid TCP option field.

Table 58: Incident Events *(continued)*

Event ID	Event Name	Description
3042	Blocked Protocol – Black-Listed DNS	DNS query has been black-listed.
3043	Bad UDP Packet – No data	UDP packet contains no data.
3044	Bad UDP Packet – Malformed	UDP header malformed.
3045	Blocked Protocol – Black-Listed AS	AS number has been black-listed.
3046	TCP Attack – HTTP Rate Flood	The protected IP is receiving GET requests at a rate higher than it is configured for.
3047	Bad ICMP Packet – Malformed	ICMP header malformed.
3048	Blocked Protocol – Black-Listed URL	URL request has been black-listed.
3049	Not Passed Thru – Unexpected Interface	Received packet came in over an unexpected interface, so it was not passed on.
3050	Bad O-IP Packet – Protocol	Invalid IP protocol number.
3051	Bad O-IP Packet – Length	IP packet is too short to contain the IP protocol header.
3052	TCP Attack – HTTP Req Incomplete	The HTTP GET request was never completed.
3053	Overloaded IP – Stall	The protected IP has stopped responding to anything.
3054	Fragment Attack – Timeout	Not all fragments seen.
3055	Fragment Attack – Repeats	ICMP packets being repeated at a rate of more than 40 per second.
3056	Fragment Attack – Bad Length	Invalid fragment length in IP header.
3057	Not Passed Thru – Keep-Alive Response	TCP response packet to internally generated keepalive probe packet has been dropped.
3058	Not Passed Thru – MAC Table Overflow	Internal table for MAC addresses is full. Oldest entry has been expired.
3059	Not Passed Thru – Packet To Us	Packet sent to an Internet or a protected interface MAC address.
3060	Not Passed Thru – Packet From Us	Packet sent by someone pretending to be an Internet or a protected interface using their MAC address.

Table 58: Incident Events *(continued)*

Event ID	Event Name	Description
3061	Not Passed Thru – Short Circuit Active	The same (source) MAC address has been seen on both sides of the DDoS Secure appliance.
3062	Not Passed Thru – Same Side	The source and destination MAC address both reside on the same side of the DDoS Secure appliance.
3063	Not Passed Thru – Probe State	Failover is in the probe state, so no traffic is passing through yet.
3064	Not Passed Thru – Standby State	Failover is in the standby state – traffic flows through other DDoS Secure appliance.
3065	Not Passed Thru – Out Of Service State	The DDoS Secure appliance processing engine is not currently running.
3066	Not Passed Thru – Deactivated	DDoS Secure appliance has detected an error and has disabled the passing of any traffic.
3067	Not Passed Thru – HeartBeat	Failover heartbeat is never passed through a DDoS Secure appliance.
3068	Overloaded IP – Backlog	The protected IP cannot keep up with new TCP connection requests.
3069	Blocked Protocol – Undefined Protected IP	Invalid Protected IP – not within the valid list of IPs.
3070	TCP Attack – No Data Xfer	No data in either direction was transferred on the TCP connection. The connection was just opened and then closed.
3071	TCP Attack – No Server Data Xfer	A webserver did not respond to a GET request.
3072	TCP Attack – Connection Rate Flood	The protected IP is receiving GET requests at a rate higher than it is configured for.
3073	Overloaded IP – Threads	The protected IP has stopped responding to new TCP requests.
3074	Bad IP Packet – Reflected Route	IP packet is being reflected off a router – same packet is passed both ways through the DDoS Secure appliance. Informational only.
3075	Not Passed Thru – BPDU Packet	Failover mode does not allow through Spanning Tree packets.
3076	Not Passed Thru – Direction Unknown	Logging-Tap only. MAC address not learned yet.
3077	Not Passed Thru – MAC Misconfigured	A MAC address has been configured for one side of the DDoS Secure appliance, but this packet with this source MAC address has been seen on the other side of the DDoS Secure appliance.
3078	TCP Attack – Port Scan	A potential port scan was detected.

Table 58: Incident Events *(continued)*

Event ID	Event Name	Description
3079	TCP Attack – Small Window	Client has closed TCP window.
3080	TCP Attack – Client Abort	Client aborted connection after request.
3081	Not Passed Thru – Generated Response	This is a response packet to a DDoS Secure generated request and is being dropped. Example is the generation of a TCP keepalive packet.
3082	Blocked Protocol – Blocked SIP	SIP request has been black-listed.
3083	TCP Attack – URL Rate Limited	DDoS Secure is rate-limiting traffic requesting this URL.
3084	UDP Attack – DNS Rate Limited	DDoS Secure is rate-limiting traffic requesting this DNS query.
3085	UDP Attack – SIP Rate Limited	DDoS Secure is rate-limiting traffic requesting this SIP.
3086	Bad TCP Packet – CheckSum	The TCP packet has an invalid checksum.
3087	TCP Attack – HTTP format	The format of the HTTP request is illegal.
3088	Unknown Session – Reflective Attack	Defending against a reflective attack where a protected IP is the target.

Table 59: Worst Offenders

Event ID	Event Name	Description
4001	Bandwidth	Bandwidth rate exceeded for MAC address, portal, or filter.
4002	Packet Rate	Packet rate exceeded for MAC address, portal, or filter. The appliance has detected high rates of small packets.
4003	Blocked Protocol – Black-Listed	This IP address has been black-listed, because it is has been defined as part of a black-listed network.
4004	Blocked Protocol – Icmp Type	No filters match for this ICMP packet.
4005	Blocked Protocol – Port	No filters match for this destination port.
4006	Blocked Protocol – Other Proto	No filters match for this protocol type.
4007	Not Passed Thru – Runt Packet	Undersized packet has been dropped.
4008	Unknown Session – Icmp Response	ICMP response packet has no matching ICMP request in the state table.
4009	Unknown Session – Icmp Diag Response	ICMP diagnostic response packet does not match a state table entry for the respective IP protocol.

Table 59: Worst Offenders *(continued)*

Event ID	Event Name	Description
4010	Unknown Session – No State	TCP packet has no state table entry and is not a SYN packet.
4011	Unknown Session – Invalid State	TCP packet has a state table entry, but packet is out of state.
4012	TCP Attack – RST	RST packet has invalid sequence number.
4013	IP Attack – Land	Source and destination IP addresses are equal.
4014	TCP Attack – Syn-Ack Timeout	The client IP did not complete the TCP connection.
4015	Blocked Protocol – Country Black-Listed	Traffic to or from a country has been blocked, because the country is black-listed.
4016	TCP Attack – Syn Flood	The protected IP is receiving SYN packets at a rate higher than it is configured for or can handle.
4017	TCP Attack – Connection Flood	The protected IP has reached its concurrent connection configured limit.
4018	TCP Attack – Table Full	Internal state table for TCP connections is being CHARM protected.
4019	Bad TCP Packet – Fast Repeat Ack	Identical packets containing ACKs are being repeated at a rate of greater than 10 per second.
4020	TCP Attack – HTTP Flood	The protected IP has reached its concurrent GET/HEAD configured limit.
4021	UDP Attack – Table Full	Internal state table for UDP information is full.
4022	Not Passed Thru – Pause Frame	Ethernet pause frame has been dropped.
4023	TCP Attack – HTTP Timeout	The protected IP did not respond to a GET/HEAD request in a timely manner.
4024	ICMP Attack – Repeats	ICMP packets being repeated at a rate of more than 40 per second.
4025	ICMP Attack – Table Full	Internal state table for ICMP is being CHARM protected.
4026	Not Passed Thru – State Sync	State synchronization packets are being processed but not passed through.
4027	Other-IP Attack – Table Full	Internal state table for Other IPs is being CHARM protected.
4028	Not Passed Thru – State Sync Sent	State synchronization packets are being processed but not passed through.
4029	Fragment Attack – Ping of Death	Assembled packet is longer than 65,535 bytes.

Table 59: Worst Offenders *(continued)*

Event ID	Event Name	Description
4030	Fragment Attack – Header Overlay	Fragment start overlays protocol header.
4031	Fragment Attack – Table Full	Internal state table for fragments is being CHARM protected.
4032	Fragment Attack – Small Size	Initial TCP fragment is smaller than header.
4033	Fragment Attack – No Fragments allowed	No fragmented packets are allowed to or from this protected IP.
4034	Bad IP Packet – Invalid Source Address	IP packet has invalid source address.
4035	Bad IP Packet – Broken Header	IP header malformed - RFC non-compliant.
4036	Bad IP Packet – Invalid Option	IP packet has invalid option field or field length.
4037	Bad IP Packet – Size Mismatch	IP packet has invalid field length.
4038	Blocked Protocol – Temp Black-Listed	This IP address has been temporarily black-listed because of its aggressive behavior.
4039	Bad TCP Packet – Flags	Invalid TCP flags combinations.
4040	Bad TCP Packet – Malformed	Format of TCP header invalid.
4041	Bad TCP Packet – Option	Invalid TCP option field.
4042	Blocked Protocol – Black-Listed DNS	DNS query has been black-listed.
4043	Bad UDP Packet – No data	UDP packet contains no data.
4044	Bad UDP Packet – Malformed	UDP header malformed.
4045	Blocked Protocol – Black-Listed AS	AS number has been black-listed.
4046	TCP Attack – HTTP Rate Flood	The protected IP is receiving GET requests at a rate higher than it is configured for.
4047	Bad ICMP Packet – Malformed	ICMP header malformed.
4048	Blocked Protocol – Black-Listed URL	URL request has been black-listed.
4049	Not Passed Thru – Unexpected Interface	Received packet came in over an unexpected interface, so it was not passed on.

Table 59: Worst Offenders *(continued)*

Event ID	Event Name	Description
4050	Bad O-IP Packet – Protocol	Invalid IP protocol number.
4051	Bad O-IP Packet – Length	IP packet is too short to contain the IP protocol header.
4052	TCP Attack – HTTP Req Incomplete	The HTTP GET request was never completed.
4053	Overloaded IP – Stall	The protected IP has stopped responding to anything.
4054	Fragment Attack – Timeout	Not all fragments seen.
4055	Fragment Attack – Repeats	ICMP packets being repeated at a rate of more than 40 per second.
4056	Fragment Attack – Bad Length	Invalid fragment length in IP header.
4057	Not Passed Thru – Keep-Alive Response	TCP response packet to internally generated keepalive probe packet has been dropped.
4058	Not Passed Thru – MAC Table Overflow	Internal table for MAC addresses is full. Oldest entry has been expired.
4059	Not Passed Thru – Packet To Us	Packet sent to Internet or protected interface MAC address.
4060	Not Passed Thru – Packet From Us	Packet sent by someone pretending to be an Internet or a protected interface using their MAC address.
4061	Not Passed Thru – Short Circuit Active	The same (source) MAC address has been seen on both sides of the DDoS Secure appliance.
4062	Not Passed Thru – Same Side	The source and destination MAC address both reside on the same side of the DDoS Secure appliance.
4063	Not Passed Thru – Probe State	Failover is in the probe state, so no traffic passing through yet.
4064	Not Passed Thru – Standby State	Failover is in the standby state— traffic flows through the other DDoS Secure appliance.
4065	Not Passed Thru – Out Of Service State	The DDoS Secure appliance processing engine is not currently running.
4066	Not Passed Thru – Deactivated	DDoS Secure appliance has detected an error and has disabled the passing of any traffic.
4067	Not Passed Thru – HeartBeat	Failover heartbeat is never passed through a DDoS Secure appliance.
4068	Overloaded IP – Backlog	The protected IP cannot keep up with new TCP connection requests.

Table 59: Worst Offenders *(continued)*

Event ID	Event Name	Description
4069	Blocked Protocol – Undefined Protected IP	Invalid protected IP—not in the valid list of IPs.
4070	TCP Attack – No Data Xfer	No data in either direction was transferred on the TCP connection. The connection was just opened and then closed.
4071	TCP Attack – No Server Data Xfer	A webserver did not respond to a GET request.
4072	TCP Attack – Connection Rate Flood	The protected IP is receiving GET requests at a rate higher than it is configured for.
4073	Overloaded IP – Threads	The protected IP has stopped responding to new TCP requests.
4074	Bad IP Packet – Reflected Route	IP packet is being reflected off a router - same packet is passed both ways through the DDoS Secure appliance. Informational only.
4075	Not Passed Thru – BPDU Packet	Failover mode does not allow through spanning tree packets.
4076	Not Passed Thru – Direction Unknown	Logging-Tap only. MAC address not learned yet.
4077	Not Passed Thru – MAC Misconfigured	A MAC address has been configured for one side of the DDoS Secure appliance, but this packet with this source MAC address has been seen on the other side of the DDoS Secure appliance.
4078	TCP Attack – Port Scan	A potential port scan was detected.
4079	TCP Attack – Small Window	Client has closed TCP window.
4080	TCP Attack – Client Abort	Client aborted connection after request.
4081	Not Passed Thru – Generated Response	This is a response packet to a DDoS Secure generated request and is being dropped. Example is the generation of a TCP keepalive packet.
4082	Blocked Protocol – Blocked SIP	SIP request has been black-listed.
4083	TCP Attack – URL Rate Limited	DDoS Secure is rate-limiting traffic requesting this URL.
4084	UDP Attack – DNS Rate Limited	DDoS Secure is rate-limiting traffic requesting this DNS query.
4085	UDP Attack – SIP Rate Limited	DDoS Secure is rate-limiting traffic requesting this SIP.
4086	Bad TCP Packet – CheckSum	The TCP packet has an invalid checksum.
4087	TCP Attack – HTTP format	The format of the HTTP request is illegal.

Table 59: Worst Offenders *(continued)*

Event ID	Event Name	Description
4088	Unknown Session – Reflective Attack	Defending against a reflective attack where a protected IP is the target.

Table 60: Temporary Black-List

Event ID	Event Name	Description
5002	Exceeded URI GET Request Rate	Worst Offender IP is temporarily black-listed, because it exceeds **show appliance autoblockgetrate**.
5003	Exceeds SYN + RST + F2D Count	Worst Offender IP is temporarily black-listed, because it exceeds **show appliance autoblocksynrst**.
5004	GUI Request	The user elected to temporarily black-list this IP address.
5005	Exceeded Fragmented Packets Timeout Rate	Worst Offender IP is temporarily black-listed, because it exceeds **show appliance autoblockfragrate**.
5006	Exceeded Irritant Rate	Worst Offender IP is temporarily black-listed, because it exceeds **show appliance autoblockratet1**.
5007	Exceeded Resource Consumption Rate	Worst Offender IP is temporarily black-listed, because it exceeds **show appliance autoblockgratet2**.

Table 61: Permanent White-List/Black-List

Event ID	Event Name	Description
6001	Black List IP(s)	IP addresses that are permanently black-listed.
6002	White List IP(s)	IP addresses that are permanently white-listed.
6003	Preferred List IP(s)	IP addresses that are permanently preferred listed (gets a CHARM boost).
6004	White No Log List IP(s)	IP addresses that are permanently white-listed but activity is not logged.
6005	No Auto Black List List IP(s)	IP addresses that are permanently flagged as not being allowed to become temporarily black-listed.
6006	Country Allow List IP(s)	IP addresses that are allowed to override any country black-list.
6007	MegaProxy List IP(s)	IP addresses that are defined as proxy servers.
6008	Default Charm List IP(s)	IP addresses that are defined as permanently having the default CHARM score.
6009	Black List AS#	AS numbers that are to be black-listed.

Table 61: Permanent White-List/Black-List *(continued)*

Event ID	Event Name	Description
6010	Black List Country	Countries that are to be black-listed.
6011	Preferred Country	Countries that are on the permanently Preferred list (gets a CHARM boost).

LEEF Extensions

Table 62 on page 236 describes the supported LEEF extensions parameter.

Table 62: LEEF Extensions Parameter

Name	Description	Attribute Type	Attribute Limits
action	Action mentioned in the event. For the DDoS Secure appliance, it indicates DROP or NOTIFY.	String	63
cat	The device event category. For the DDoS Secure appliance, it indicates the type of incident message. The values are START, END, or ONGOING.	String	1023
CurrentPps	The current packets per seconds (PPS) that are being observed.	Integer	0 to 4294967295
desc	Description of the event ID.	String	255
devTime	The time when event started.	Timestamp	
devTimeFormat	Specifies the format of the time.	String	
dir	Indicates the direction that the packets are flowing. 0 == Inbound.	0 or 1	
dst	The IP address of the event destination.	IPv4 or IPv6 address	
dstPort	The destination port of the event.	Integer	0 to 65535
end	Time the event finishes.	String	255

Table 62: LEEF Extensions Parameter *(continued)*

Name	Description	Attribute Type	Attribute Limits
entity	The zone category of incident that is being reported. This provides information on what zone the incident was detected in. The choices are MAC, IP, PORTAL, FILTER, URL, DNS, SIP, BLACKLIST.	String	255
id	Incident ID.	String	255
identSrc	The source IP address of an event. This will be included if identHostName is included.	IPv4 or IPv6 address	
identHostName	The host name of the source. This will be used to specify the TEID of a source.	String	255
msg	Associated message	String	255
PeakBps	The peak bytes per second (BPS) that have been observed.	Integer	0 to 4294967295
PeakPps	The peak packets per second (PPS) that have been observed.	Integer	0 to 4294967295
proto	Transport protocol of the event.	String	255
resource	This field indicates the type of resource that is being reported on.	String	255
realm	The portal name associated with the event. It is only included with the message for certain event types.	String	255
sev	Numeric value that indicates the severity of the event. 1 is the lowest and 10 is the highest.	Integer	1-10
src	The IP address of the event source.	IPv4 or IPv6 address	
srcPort	The source port of the event.	Integer	0 to 65535

Table 62: LEEF Extensions Parameter *(continued)*

Name	Description	Attribute Type	Attribute Limits
totalPackets	The number of packets that have been seen from the event source.	Integer	0 to 4294967295
usrName	The account name associated with the event. It is only included with the message for certain event types.	String	255
url	If present, provides extra information on why the request was blocked.	String	255

Arcsight Extensions

Table 63 on page 238 describes the supported Arcsight Extensions parameter.

Table 63: Arcsight Extensions Parameter

Name	Description	Attribute Type	Attribute Limits
act	Action mentioned in the event. For the DDoS Secure appliance, it indicates DROP or NOTIFY.	String	63
cat	The device event category. For the DDoS Secure appliance, it indicates the type of incident message. The values are START, END, or ONGOING.	String	1023
cnt	The total count of incidents for this protected resource.	Integer	0 to 4294967295
cn1	Custom field for DDoS Secure. cn1Label is set to CurrentPps to indicate that this field is the current packets per second (PPS) that are being observed.	Integer	0 to 4294967295
cn1Label	Custom field for DDoS Secure. This is set to CurrentPps to indicate that the cn1 field is the current PPS.	String	
cn2	Custom field for DDoS Secure. cn2Label is set to PeakPps to indicate that this field is the peak PPS.	Integer	0 to 4294967295

Table 63: Arcsight Extensions Parameter *(continued)*

Name	Description	Attribute Type	Attribute Limits
cn2Label	Custom field for DDoS Secure. This is set to PeakPps to indicate that the cn2 field is the peak PPS.	String	
cn3	Custom field for DDoS Secure. cn3Label is set to PeakBps to indicate that this field is the peak bytes per second (Bps) that are being observed.	Integer	0 to 4294967295
cn3Label	Custom field for DDoS Secure. This is set to PeakBps to indicate that the cn1 field is the current PPS.	String	
cs1	Custom field for DDoS Secure. The field cs1Label is set to Entity. This field indicates the zone category of incident that is being reported. This provides information on what zone the incident was detected in. The choices are MAC, IP, PORTAL, FILTER, URL, DNS, SIP, BLACKLIST.	String	255
cs1Label	Set to Entity to indicate that cs1 is the entity field.	String	255
cs2	Custom field for DDoS Secure. The field cs2Label is set to Resource. This field indicates the type of resource that is being reported on.	String	255
cs2Label	Set to Resource to indicate that cs2 is the entity field.	String	255
c6a2	The source IPv6 address of a device.	IPv6 address	
c6a2Label	Set to SrcIP to indicate that c6a2 is the IPv6 source address.		
c6a3	The destination IPv6 address of a device.	IPv6 address	
c6a3Label	Set to DstIP to indicate that c6a3 is the IPv6 destination address.		

Table 63: Arcsight Extensions Parameter *(continued)*

Name	Description	Attribute Type	Attribute Limits
deviceDirection	Indicates the direction that the packets are flowing.	0 or 1	
deviceFacility	The syslog facility generating this event.	String	255
dpt	The destination port of the event.	Integer	0 to 65535
dst	The IP address of the event destination.	IPv6 Address	
duser	The account name associated with the event. It is only included with the message for certain event types.	String	255
dvc	The source IP address of device. This will be included if dvchost is included.	IPv4 or IPv6 address	
dvchost	The host name of the device. This will be used to specify the TEID of a source.	String	63
externalId	Incident ID.	String	255
msg	The description of the event.	String	1023
proto	Transport protocol of the event.	String	
request	If present, provides extra information on why the request was blocked.	String	255
spt	The source port of the event.	Integer	0 to 65535
src	The IP address of the event source.	IPv4 Address	
start	The time when the event started.	Time Stamp	

General Messages

CEF Message Format

Apr 6 11:55:40 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|1034|Health Check|4|deviceFacility=local6 msg=Peak Usage: Sat Apr 5 12:10:31

```
Appliances: 1 Licensed: 1G Direction: Outbound Peak Rate: 127M
```

LEEF Message Format

```
Apr 6 11:44:21 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
1034| desc=Health Check sev=4 msg=Peak Usage: Sat Apr 5 12:10:31
Appliances: 1 Licensed: 1G Direction: Outbound Peak Rate: 127M
```

Incident Messages

Incident message – Beginning Message

CEF Message Format

```
Apr 7 17:55:35 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
3016|TCP Attack - Syn Flood|4|externalId=20140407/009107
cs1=111.91.236.136/-General-/IP cs1Label=Entitycs2=Backlog Queue
cs2Label=ResourcedeviceDirection=0 src=183.225.1.56 dst=111.91.236.136
proto=TCP dpt=80 cat=START start=Apr 07 2014 17:55:27 cn2=1545
cn2Label=PeakPps cnt=8201 act=NOTIFY
```

LEEF Message Format

```
Apr 7 17:58:41 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
3084|desc=UDP Attack - DNS Rate Limited sev=4 id=20140407/011428
entity=111.91.237.115/-General-/DNS resource=gerdar3.ru.?ANY proto=UDP
scrPort=59905 dstPort=53 dir=inbound src=37.60.61.86 dst=111.91.237.115
cat=START devTime=2014-04-07 17:58:32 devTimeFormat=yyyy-MM-dd
HH:mm:ss CurrentPps=114 PeakPps=123 totalPackets=896 realm=-General- action=DROP
```

Incident message – Status Update message

CEF Message Format

```
Apr 7 17:55:41 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
3016|TCP Attack - Syn Flood|4|externalId=20140407/009107
cs1=111.91.236.136/-General-/IP cs1Label=Entitycs2=Backlog Queue
cs2Label=ResourcedeviceDirection=0 src=108.163.215.181 dst=111.91.236.136
proto=TCP dpt=80 cat=ONGOING start=Apr 07 2014 17:55:27 cn2=2010
cn2Label=PeakPps cnt=16458 act=NOTIFY
```

LEEF Message Format

```
Apr 7 17:58:47 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
3084|desc=UDP Attack - DNS Rate Limited sev=4 id=20140407/011428
entity=111.91.237.115/-General-/DNS resource=gerdar3.ru.?ANY proto=UDP
scrPort=11464 dstPort=53 dir=inbound src=37.60.61.86 dst=111.91.237.115
cat=ONGOING devTime=2014-04-07 17:58:32 devTimeFormat=yyyy-MM-dd
HH:mm:ss CurrentPps=72 PeakPps=123 totalPackets=1488 realm=-General- action=DROP
```

Incident message – End Message

CEF Message Format

```
Apr 7 17:56:18 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
3084|UDP Attack - DNS Rate Limited|4|externalId=20140407/009097
cs1=111.91.237.115/-General-/DNS cs1Label=Entitycs2=gerdar3.ru.?ANY
cs2Label=ResourcedeviceDirection=0 src=37.60.61.86 dst=111.91.237.115
proto=UDP dpt=53 cat=END start=Apr 07 2014 17:55:26 end=Apr 07 2014
17:55:44 cn2=186 cn2Label=PeakPps cnt=2525 act=NOTIFY
```

LEEF Message Format

```
Apr 7 17:59:35 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
3016|desc=TCP Attack - Syn Flood sev=4 id=20140407/011439
entity=111.91.236.136/-General-/IP resource=Backlog Queue proto=TCP
scrPort=51203 dstPort=80 dir=inbound src=108.163.215.175
dst=111.91.236.136 cat=END devTime=2014-04-07 17:58:34
devTimeFormat=yyyy-MM-dd HH:mm:ss CurrentPps=0 PeakPps=1435
totalPackets=25602 realm=-General- action=DROP
```

Worst Offender Messages

Worst Offender Message – Start Message

CEF Message Format

```
Apr 7 17:55:26 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
4001|Bandwidth - Rate Limited|4|src=37.60.61.86 dst=111.91.237.189
proto=UDP spt=35596 dpt=53 cat=START start=Apr 07 2014 17:55:26 cn1=65
cn1Label=CurrentPps cn2=65 cn2Label=PeakPps cnt=131 duser=-General- act=DROP
```

LEEF Message Format

```
Apr 7 17:58:34 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
4084|desc=UDP Attack - DNS Rate Limited sev=4 proto=UDP
scrPort=21252 dstPort=53 src=37.60.61.86 dst=111.91.237.115 cat=START
devTime=2014-04-07 17:58:32 devTimeFormat=yyyy-MM-dd HH:mm:ss
CurrentPps=331 PeakPps=331 totalPackets=663 realm=-General- action=DROP
```

Worst Offender Message – End Message

CEF Message Format

```
Apr 7 17:56:18 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
4001|Bandwidth - Rate Limited|4|src=117.200.146.45 dst=103.2.13.87
proto=TCP spt=3034 dpt=445 cat=END start=Apr 07 2014 17:55:44 end=Apr 07
2014 17:55:44 cn1=0 cn1Label=CurrentPps cn2=29 cn2Label=PeakPps cnt=114
duser=-General- act=DROP
```

LEEF Message Format

```
Apr 7 17:58:34 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
4084|desc=UDP Attack - DNS Rate Limited sev=4 proto=UDP
scrPort=21252 dstPort=53 src=37.60.61.86 dst=111.91.237.115 cat=END
devTime=2014-04-07 17:58:32 devTimeFormat=yyyy-MM-dd HH:mm:ss
```

```
CurrentPps=331 PeakPps=331 totalPackets=663 realm=-General-
action=DROP
```

Temporary Black-List Messages

Temporary Black List Message – Start Message

CEF Message Format

```
Apr 7 17:55:48 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
5003|Exceeds SYN + RST + F2D Count|7|src=190.57.152.142
dst=255.255.255.255 proto=TCP spt=3536 dpt=5000 cat=START start=Apr 07 2014
17:55:47 cn1=100 cn1Label=CurrentPps cn2=100 cn2Label=PeakPps cn3=58904
cn3Label=PeakBps cnt=200 duser=-General- act=DROP
```

LEEF Message Format

```
Apr 7 17:59:04 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
5007|desc=Exceeded Resource Consumption Rate sev=7 proto=UDP
scrPort=31254 dstPort=53 src=37.60.61.86 dst=255.255.255.255 cat=START
devTime=2014-04-07 17:59:02 devTimeFormat=yyyy-MM-dd HH:mm:ss
CurrentPps=382 PeakPps=382 PeakBps=247256 totalPackets=764 realm=-
General- action=DROP
```

Temporary Black List Message – End Message

CEF Message Format

```
Apr 7 17:56:18 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
5007|Exceeded Resource Consumption Rate|6|src=37.60.61.86
dst=255.255.255.255 proto=UDP spt=60183 dpt=53 cat=END start=Apr 07 2014
17:55:44 end=Apr 07 2014 17:55:47 cn1=0 cn1Label=CurrentPps cn2=508
cn2Label=PeakPps cn3=328840 cn3Label=PeakBps cnt=1674 duser=-General-act=DROP
```

LEEF Message Format

```
Apr 7 17:59:35 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
5007|desc=Exceeded Resource Consumption Rate sev=6 proto=UDP
scrPort=60183 dstPort=53 src=37.60.61.86 dst=255.255.255.255 cat=END
devTime=2014-04-07 17:59:02 devTimeFormat=yyyy-MM-dd HH:mm:ss
CurrentPps=0 PeakPps=382 PeakBps=247256 totalPackets=891 realm=-
General- action=DROP
```

Permanent Black-List/White-List Messages

These messages are sent out every time there is a configuration change or once an hour.

CEF Message Format

```
Apr 7 17:55:54 ws_192_168_0_189 CEF: 0|Juniper|DDoS Secure|5.13.2-2a|
6007|MegaProxy List IP(s)|4|externalId=1396889754 msg=1.2.3.4,4.5.6.7
```

LEEF Message Format

```
Apr 7 17:59:08 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2a|
6002|desc=White List IP(s) sev=4 id=1396889947 catmsg=1.2.3.5,4.5.6.0/24
```

Multiline example:

```
Apr 17 17:12:45 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2d|
6001|desc=Black List IP(s) sev=4 id=1397751165 msg=1.2.3.6/31,1.100.100.1,
1.100.101.1,1.100.102.1,1.100.103.1,1.100.104.1,1.100.105.1,1.100.106.1,1.100.107.1,
1.100.108.1,1.100.109.1,1.100.110.1,1.100.111.1,1.100.112.1,1.100.113.1,1.100.114.1,
1.100.115.1,1.100.116.1,1.100.117.1,1.100.118.1,1.100.119.1,1.100.120.1,1.100.121.1,
1.100.122.1,1.100.123.1,1.100.124.1,1.100.125.1,1.100.126.1,1.100.127.1,1.100.128.1,
1.100.129.1,1.100.130.1,1.100.131.1,1.100.132.1,1.100.133.1,1.100.134.1,1.100.135.1,
1.100.136.1,1.100.137.1,1.100.138.1,1.100.13139.1,1.100.140.1,1.100.141.1,1.100.142.1,
1.100.143.1,1.100.144.1,1.100.145.1,1.100.146.1,1.100.147.1,1.100.148.1,1.100.149.1,
1.100.150.1,1.100.151.1,1.100.152.1,1.100.153.1,1.100.154.1,1.100.155.1,1.100.156.1,
1.100.157.1,1.100.158.1,1.100.159.1,1.100.160.1,1.100.161.1,1.100.162.1,1.100.163.1,
1.100.164.1,1.100.165.1,1.100.166.1,1.100.167.1,1.100.168.1,1.100.169.1,1.100.170.1,
1.100.171.1,1.100.172.1,1.100.173.1
Apr 17 17:12:45 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2d|
6001|desc=Black List IP(s) sev=4 id=1397751165 msg=1.100.174.1,1.100.175.1,
1.100.176.1,1.100.177.1,1.100.178.1,1.100.179.1,1.100.180.1,
1.100.181.1,1.100.182.1,1.100.183.1,1.100.184.1,1.100.185.1,1.100.186.1,
1.100.187.1,1.100.188.1,1.100.189.1,1.100.190.1,1.100.191.1,1.100.192.1,1.100.193.1,
1.100.194.1,1.100.195.1,1.100.196.1,1.100.197.1,1.100.198.1,1.100.199.1,1.100.200.1,
1.100.201.1,1.100.202.1,1.100.203.1,1.100.204.1,1.100.205.1,1.100.206.1,1.100.207.1,
1.100.208.1,1.100.209.1,1.100.210.1,1.100.211.1,1.100.212.1,1.100.213.1,1.100.214.1,
1.100.215.1,1.100.216.1,1.100.217.1,1.100.218.1,1.100.219.1,1.100.220.1,1.100.221.1,
1.100.222.1,1.100.223.1,1.100.224.1,1.100.225.1,1.100.226.1,1.100.227.1,1.100.228.1,
1.100.229.1,1.100.230.1,1.100.231.1,1.100.232.1,1.100.233.1,1.100.234.1,1.100.235.1,
1.100.236.1,1.100.237.1,1.100.238.1,1.100.239.1,1.100.240.1,1.100.241.1,1.100.242.1,
1.100.243.1,1.100.244.1,1.100.245.1,1.100.246.1,1.100.247.1,1.100.248.1
Apr 17 17:12:45 ws_192_168_0_189 LEEF: 1.0|Juniper|DDoS Secure|5.13.2-2d|
6001|desc=Black List IP(s) sev=4 id=1397751165 msg=1.100.249.1,1.100.250.1,
1.100.251.1,1.100.252.1,1.100.253.1,1.100.254.1,1.100.255.1,4.5.6.7
```

Related Documentation

- Starting a CLI Session on page 5
- Navigating Through the CLI on page 7
- Changing the Configuration Using the CLI on page 8

APPENDIX C

DDoS Secure Appliance TCP States

Understanding TCP States

Table 64 on page 245 provides the details of TCP states held by DDoS Secure appliance during operation. The parameters correspond approximately to the standard states held by a conventional TCP device, but are subdivided due to the unique method of handling connections by the appliance.

Table 64: TCP Status Details

Parameter	Description
SYN	Client has sent a SYN.
SPF	Client has sent a SYN to an internally filtered port.
SIF	Client has sent a SYN to an internally filtered IP address.
S-A	Server has responded with SYN-ACK.
S-S	Client and server SYN.
ACK	Connection established, but no data from client or server.
P-A	Client sent data, server did not acknowledged any data.
GET	Currently processing an HTTP GET/HEAD/POST request.
EST	Connection established, data is flowing.
F1S	Internet has sent a FIN.
F2S	Protected ACKd FIN.
F3S	Internet sent FIN, protected ACKd FIN and has sent its own FIN.
F-F	Internet and protected sent FIN, but neither ACKd FIN.

Table 64: TCP Status Details *(continued)*

Parameter	Description
F1D	Protected has sent a FIN.
F2D	Internet has ACKd FIN.
F3D	Protected sent FIN, Internet ACKd FIN and sent its own FIN.
CLS	Closed (All FINs ACKd).
RST	RESET (either end) to SYN.
R-C	RESET (either end) to force session close.
UNK	Session in unknown state.
GETs	Count of connections processing a GET/HEAD request.

Related Documentation

- Understanding ICMP Types on page 247
- Understanding Index Attack Types on page 249

APPENDIX D

ICMP Types

Understanding ICMP Types

Table 65 on page 247 provides ICMPv4 details.

Table 65: ICMPv4 Details

Parameter	Description
Echo Reply	0
Destination Unreachable	3
Source Quench	4
Redirect (change route)	5
Echo Request	8
Time Exceeded	11
Parameter Problem	12
Timestamp Request	13
Timestamp Reply	14
Information Request	15
Information Reply	16
Address Mask Request	17
Address Mask Reply	18

Table 66 on page 248 provides ICMPv6 details.

Table 66: ICMPv6 Details

Parameter	Description
Destination Unreachable	1
Packet Too Big	2
Time Exceeded	3
Parameter Problem	4
Echo Request	128
Echo Reply	129
Group Membership Query	130
Group Membership Reply	131
Group Membership Reduction	132
Router Solicitation	133
Router Advertisement	134
Neighbor Solicitation	135
Neighbor Advertisement	136
Redirect	137

Related Documentation

- Understanding TCP States on page 245
- Understanding Index Attack Types on page 249

APPENDIX E

Incident (Attack) Types

Understanding Index Attack Types

Table 67 on page 249 provides type code details.

Table 67: Type Code Details

Field	Description
-2	Recorded in auto black-list.
-1	Packets not dropped, not recorded in worst offenders.
0	Not recorded in worst offenders.
1	Irritant attacks used by worst offenders and auto black-list.
2	Resource consuming attacks – used by worst offenders and auto black-list.

Table 68 on page 249 provides attack type code details.

Table 68: Attack Type Details

Attack Type	Type	Details
Bad ICMP Packet – Malformed	1	ICMP header malformed (length, options, and so on).
Bad IP Packet - Broken Header	1	IP address header malformed – RFC non-compliant.
Bad IP Packet - Invalid Option	1	IP address packet has invalid option field or field length.
Bad IP Packet - Invalid Source Address	0	IP address packet has invalid source address.
Bad IP Packet - Reflected Route	-1	IP address packet is being reflected off a router – same packet is passed both ways through the DDoS Secure appliance. Informational only.
Bad IP Packet - Size Mismatch	1	IP address packet has invalid field length.

Table 68: Attack Type Details *(continued)*

Attack Type	Type	Details
Bad O-IP Packet - Length	1	IP address packet too short to contain IP address protocol header.
Bad O-IP Packet - Protocol	1	Invalid IP address protocol number.
Bad TCP Packet - Fast Repeat Ack	0	Identical packets containing ACKs are being repeated at a rate of greater than 10 per second.
Bad TCP Packet - Flags	1	Invalid TCP flag combinations.
Bad TCP Packet - Malformed	1	Format of TCP header invalid.
Bad TCP Packet - Option	1	Invalid TCP option field.
Bad UDP Packet - Malformed	1	UDP header malformed.
Bad UDP Packet - No data	1	UDP packet contains no data.
Bandwidth - Rate Limited	2	Bandwidth rate exceeded for MAC address/portal/filter.
Blocked Protocol – Black-Listed	0	This IP address is black-listed as it is part of a black-listed network.
Blocked Protocol – Black-Listed AS	0	AS is blocked.
Blocked Protocol – Black-Listed DNS	1	DNS query is blocked.
Blocked Protocol - Black-Listed SIP	1	SIP request is blocked.
Blocked Protocol – Black-Listed URL	1	URL request is blocked.
Blocked Protocol – Country Black-Listed	0	Traffic to and from country is blocked.
Blocked Protocol - Icmp Type	1	No filters match for this ICMP packet.
Blocked Protocol – Other Proto	1	No filters match for this protocol type.
Blocked Protocol - Port	1	No filter match for this destination port.
Blocked Protocol – Temp Black-Listed	-2	This IP address is temporarily black-listed.
Blocked Protocol–Undefined protected IP	0	Traffic to or from an address that is not defined as a protected IP address.
Fragment Attack - Bad Length	2	Invalid fragment length in IP address header.
Fragment Attack - Header Overlay	2	Fragment start overlays protocol header.

Table 68: Attack Type Details *(continued)*

Attack Type	Type	Details
Fragment Attack - No Fragments allowed	1	Fragmentation is disabled in the filter.
Fragment Attack - Ping of Death	2	Assembled packet is longer than 65,535 bytes.
Fragment Attack – Repeats	1	Same fragment is sent again.
Fragment Attack – Small Size	2	Initial TCP fragment is smaller than header.
Fragment Attack – Table Full	1	Internal state table for fragments is full.
Fragment Attack – Timeout	2	Not all fragments seen.
ICMP Attack - Repeats	1	ICMP packets being repeated at a rate of more than 40 per second.
ICMP Attack - Table Full	1	Internal state table for ICMP is full.
IP Attack - Land	2	Source and destination IP addresses are equal.
Not Passed Thru – BPDU Packet	0	Failover mode does not allow through spanning tree packets.
Not Passed Thru – Deactivated	0	DDoS Secure appliance has operationally closed down.
Not Passed Thru – Direction Unknown	0	Logging-tap only. MAC address not obtained yet.
Not Passed Thru – Generated Response	0	ARP packet generated by redirect server.
Not Passed Thru - HeartBeat	0	Failover heartbeat is never passed through a DDoS Secure appliance.
Not Passed Thru - Keep-Alive Response	0	TCP response packet to internally generated keepalive probe packet is dropped.
Not Passed Thru - MAC Misconfigured	0	A MAC address is configured for one side of DDoS Secure appliance, but this packet with this source MAC address is seen on the wrong side of the DDoS Secure appliance.
Not Passed Thru - MAC Table Overflow	0	Internal table for MAC addresses is full. Oldest entry is expired.
Not Passed Thru - Out Of Service State	0	Failover device is out of service. No packets passing through.
Not Passed Thru - Packet From Us	0	Packet sent by someone pretending to be an Internet or a protected interface by using their MAC address.
Not Passed Thru - Packet To Us	0	Packet sent to Internet or protected interface MAC address.
Not Passed Thru - Pause Frame	0	Ethernet pause frame is dropped.

Table 68: Attack Type Details *(continued)*

Attack Type	Type	Details
Not Passed Thru - Probe State	0	Failover is in the probe state, so no traffic passing through yet.
Not Passed Thru – Runt Packet	0	Undersized packet is dropped.
Not Passed Thru - Same Side	0	The source and destination MAC addresses both reside on the same side of the DDoS Secure appliance.
Not Passed Thru - Short Circuit Active	0	The same (source) MAC address is seen on both sides of the DDoS Secure appliance.
Not Passed Thru - Standby State	0	Failover is in the standby state – traffic flows through other DDoS Secure appliance.
Not Passed Thru – State Sync	0	State synchronization packets are being processed but not passed through.
Not Passed Thru – State Sync Sent	0	State synchronization packets are being processed but not passed through.
Other-IP Attack - Table Full	1	Internal state table for other IP address protocols is full. Oldest entry is expired.
Overloaded IP - Backlog	1	The protected IP address cannot keep up with new TCP connection requests.
Overloaded IP - Stall	1	The protected IP address has stopped responding to anything.
Overloaded IP - Threads	2	The protected IP address has stopped responding to new HTTP GET requests.
Packet Rate - Rate Limited	2	Packet rate exceeded as defined in a filter or portal.
TCP Attack – Client Abort	1	Client aborted connection after request.
TCP Attack - Connection Flood	2	The protected IP address has reached its concurrent connection configured limit.
TCP Attack - Connection Rate Flood	2	The protected IP address is receiving connection requests at a rate higher than it is configured for.
TCP Attack - HTTP Flood	2	The protected IP address has reached its concurrent GET/HEAD configured limit.
TCP Attack - HTTP Format	2	HTTP packet incorrectly formatted.
TCP Attack – HTTP Rate Flood	2	The protected IP address is receiving GET requests at a rate higher than it is configured for.
TCP Attack - HTTP Req Incomplete	2	The HTTP GET request was never completed.

Table 68: Attack Type Details *(continued)*

Attack Type	Type	Details
TCP Attack - HTTP Timeout	1	The protected IP address did not respond to a GET/HEAD request in a timely manner.
TCP Attack – No Data Xfer	1	No data in either direction was transferred on the TCP connection. The connection was just opened and then closed.
TCP Attack – No Server Data Xfer	1	A webserver did not respond to a GET request. Usually seen when an IP addresses is requested in the host: header field, instead of a domain name.
TCP Attack – Port Scan	2	A potential port scan was detected.
TCP Attack – RST	1	RST packet has invalid sequence number.
TCP Attack – Small Window	2	Client has closed TCP window.
TCP Attack - Syn-Ack Timeout	2	The client IP address did not complete the TCP connection.
TCP Attack - Syn Flood	2	The protected IP address is receiving SYN packets at a rate higher than it is configured for or can handle.
TCP Attack - Table Full	1	Internal state table for TCP connections is full.
UDP Attack - DNS Rate Limited	2	DNS queries are not being responded to quickly enough.
UDP Attack - SIP Rate Limited	2	SIP queries are not being responded to quickly enough.
UDP Attack - Table Full	1	Internal state table for UDP information is full.
Unknown Session - Icmp Diag Response	1	ICMP diagnostic response packet does not match a state table entry for the respective IP address protocol.
Unknown Session - Icmp Response	1	ICMP response packet has no matching ICMP request in state table.
Unknown Session - Invalid State	1	TCP packet has a state table entry, but packet is out of state (sequence numbers mismatch, or incorrect TCP flags).
Unknown Session - No State	1	TCP packet has no state table entry and is not a SYN (start of connection) packet.
Unknown Session - Reflective Attack	1	Unknown response packets to queries not initiated by a protected IP.

APPENDIX F

Letter Country Codes

DDoS Secure Appliance Country Codes

Table 69 on page 255 and Table 70 on page 256 provides the details of DDoS Secure appliance that are sort by codes.

Table 69: Code Type Details

Code	Type	Details
---	--Unknown—	
-bc	---Broadcast---	Cannot be blocked
-bl	---Black List---	Always is blocked
-bo	---Bogon address---	
-ca	---Country Allow ---	
-ce	---Class E---	
-dc	---Default CHARM---	
-lo	---Loopback---	
-mc	---Multicast---	Cannot be blocked
-mp	---Mega Proxy---	Cannot be blocked
-nb	---No Auto Block---	
-pl	---Preferred List---	
-pr	---RFC1918 address---	
-u1	---User Defined #1---	

Table 69: Code Type Details *(continued)*

Code	Type	Details
-u2	---User Defined #2---	
-u3	---User Defined #3---	
-u4	---User Defined #4---	
-u5	---User Defined #5---	
-u6	---User Defined #6---	
-u7	---User Defined #7---	
-u8	---User Defined #8---	
-u9	---User Defined #9---	
-wl	---White-list---	Cannot be blocked
-wn	---White No Log---	Cannot be blocked

Table 70: Sort by Country

Code	Details
A1	Anonymous Proxy
A2	Satellite Provider
ABW	Aruba
AFG	Afghanistan
AGO	Angola
AIA	Anguilla
ALA	Aland Islands
ALB	Albania
AND	Andorra
ANT	Netherlands Antilles
AP	Asia/Pacific Region
AQ	Antarctica

Table 70: Sort by Country *(continued)*

Code	Details
ARE	United Arab Emirates
ARG	Argentina
ARM	Armenia
ASM	American Samoa
ATG	Antigua and Barbuda
AUS	Australia
AUT	Austria
AZE	Azerbaijan
BDI	Burundi
BEL	Belgium
BEN	Benin
BFA	Burkina Faso
BGD	Bangladesh
BGR	Bulgaria
BHR	Bahrain
BHS	Bahamas
BIH	Bosnia and Herzegovina
BLR	Belarus
BLZ	Belize
BMU	Bermuda
BOL	Bolivia
BRA	Brazil
BRB	Barbados
BRN	Brunei Darussalam

Table 70: Sort by Country *(continued)*

Code	Details
BTN	Bhutan
BV	Bouvet Island
BWA	Botswana
CAF	Central African Republic
CAN	Canada
CC	Cocos (Keeling) Islands
CHE	Switzerland
CHL	Chile
CHN	China
CIV	Côte d’Ivoire
CMR	Cameroon
COD	Congo, The Democratic Republic of the
COG	Congo
COK	Cook Islands
COL	Colombia
COM	Comoros
CPV	Cape Verde
CRI	Costa Rica
CUB	Cuba
CX	Christmas Island
CYM	Cayman Islands
CYP	Cyprus
CZE	Czech Republic
DEU	Germany

Table 70: Sort by Country *(continued)*

Code	Details
DJI	Djibouti
DMA	Dominica
DNK	Denmark
DOM	Dominican Republic
DZA	Algeria
ECU	Ecuador
EGY	Egypt
ERI	Eritrea
ESH	Western Sahara
ESP	Spain
EST	Estonia
ETH	Ethiopia
EU	Europe
FIN	Finland
FJI	Fiji
FLK	Falkland Islands (Malvinas)
FRA	France
FRO	Faroe Islands
FSM	Micronesia, Federated States of
FX	France, Metropolitan
GAB	Gabon
GBR	United Kingdom
GEO	Georgia
GGY	Guernsey

Table 70: Sort by Country *(continued)*

Code	Details
GHA	Ghana
GIB	Gibraltar
GIN	Guinea
GLP	Guadeloupe
GMB	Gambia
GNB	Guinea-Bissau
GNQ	Equatorial Guinea
GRC	Greece
GRD	Grenada
GRL	Greenland
GS	South Georgia and the South Sandwich Islands
GTM	Guatemala
GUF	French Guiana
GUM	Guam
GUY	Guyana
HKG	Hong Kong
HM	Heard Island and McDonald Islands
HND	Honduras
HRV	Croatia
HTI	Haiti
HUN	Hungary
IDN	Indonesia
IMN	Isle of Man
IND	India

Table 70: Sort by Country *(continued)*

Code	Details
IO	British Indian Ocean Territory
IRL	Ireland
IRN	Iran, Islamic Republic of
IRQ	Iraq
ISL	Iceland
ISR	Israel
ITA	Italy
JAM	Jamaica
JEY	Jersey
JOR	Jordan
JPN	Japan
KAZ	Kazakhstan
KEN	Kenya
KGZ	Kyrgyzstan
KHM	Cambodia
KIR	Kiribati
KNA	Saint Kitts and Nevis
KOR	Korea, Republic of
KWT	Kuwait
LAO	Lao People’s Democratic Republic
LBN	Lebanon
LBR	Liberia
LBY	Libyan Arab Jamahiriya
LCA	Saint Lucia

Table 70: Sort by Country *(continued)*

Code	Details
LIE	Liechtenstein
LKA	Sri Lanka
LSO	Lesotho
LTU	Lithuania
LUX	Luxembourg
LVA	Latvia
MAC	Macau
MAR	Morocco
MCO	Monaco
MDA	Moldova, Republic of
MDG	Madagascar
MDV	Maldives
MEX	Mexico
MHL	Marshall Islands
MKD	Macedonia
MLI	Mali
MLT	Malta
MMR	Myanmar
MNE	Montenegro
MNG	Mongolia
MNP	Northern Mariana Islands
MOZ	Mozambique
MRT	Mauritania
MSR	Montserrat

Table 70: Sort by Country *(continued)*

Code	Details
MTQ	Martinique
MUS	Mauritius
MWI	Malawi
MYS	Malaysia
NAM	Namibia
NCL	New Caledonia
NER	Niger
NFK	Norfolk Island
NGA	Nigeria
NIC	Nicaragua
NIU	Niue
NLD	Netherlands
NOR	Norway
NPL	Nepal
NRU	Nauru
NZL	New Zealand
O1	Other
OMN	Oman
PAK	Pakistan
PAN	Panama
PCN	Pitcairn Islands
PER	Peru
PHL	Philippines
PLW	Palau

Table 70: Sort by Country *(continued)*

Code	Details
PNG	Papua New Guinea
POL	Poland
PRI	Puerto Rico
PRK	Korea, Democratic People’s Republic of
PRT	Portugal
PRY	Paraguay
PSE	Palestinian Territory
PYF	French Polynesia
QAT	Qatar
REU	Reunion
ROU	Romania
RUS	Russian Federation
RWA	Rwanda
SAU	Saudi Arabia
SDN	Sudan
SEN	Senegal
SGP	Singapore
SHN	Saint Helena
SJM	Svalbard and Jan Mayen
SLB	Solomon Islands
SLE	Sierra Leone
SLV	El Salvador
SMR	San Marino
SOM	Somalia

Table 70: Sort by Country *(continued)*

Code	Details
SPM	Saint Pierre and Miquelon
SRB	Serbia
STP	Sao Tome and Principe
SUR	Suriname
SVK	Slovakia
SVN	Slovenia
SWE	Sweden
SWZ	Swaziland
SYC	Seychelles
SYR	Syrian Arab Republic
TCA	Turks and Caicos Islands
TCD	Chad
TF	French Southern Territories
TGO	Togo
THA	Thailand
TJK	Tajikistan
TKL	Tokelau
TKM	Turkmenistan
TLS	Timor-Leste
TON	Tonga
TTO	Trinidad and Tobago
TUN	Tunisia
TUR	Turkey
TUV	Tuvalu

Table 70: Sort by Country *(continued)*

Code	Details
TWN	Taiwan
TZA	Tanzania, United Republic of
UGA	Uganda
UKR	Ukraine
UM	United States Minor Outlying Islands
URY	Uruguay
USA	United States
UZB	Uzbekistan
VAT	Holy See (Vatican City State)
VCT	Saint Vincent and the Grenadines
VEN	Venezuela
VGB	Virgin Islands, British
VIR	Virgin Islands, U.S.
VNM	Vietnam
VUT	Vanuatu
WLF	Wallis and Futuna
WSM	Samoa
YEM	Yemen
YT	Mayotte
ZAF	South Africa
ZMB	Zambia
ZWE	Zimbabwe

Table 71 on page 267 and Table 72 on page 268 provides the details of DDoS Secure appliance that are sort by country.

Table 71: Sort by Code

-bl	---Black List---	Always is blocked
-bo	---Bogon address---	
-bc	---Broadcast---	Cannot be blocked
-ca	---Country Allow---	
-ce	---Class E---	
-dc	---Default CHARM---	
-lo	---Loopback---	
-mc	---Multicast---	Cannot be blocked
-mp	---Mega Proxy---	Cannot be blocked
-nb	---No Auto Block---	
-pt	---Pen Test List---	
-pl	---Preferred List---	
-pr	---RFC1918 address---	
-u1	---User Defined #1---	
-u2	---User Defined #2---	
-u3	---User Defined #3---	
-u4	---User Defined #4---	
-u5	---User Defined #5---	
-u6	---User Defined #6---	
-u7	---User Defined #7---	
-u8	---User Defined #8---	
-u9	---User Defined #9---	
-wl	---White List---	Cannot be blocked
-wn	---White No Log---	Cannot be blocked
---	--Unknown--	

Table 72: Sort by Country

AFG	Afghanistan
ALA	Aland Islands
ALB	Albania
DZA	Algeria
ASM	American Samoa
AND	Andorra
AGO	Angola
AIA	Anguilla
A1	Anonymous Proxy
AQ	Antarctica
ATG	Antigua and Barbuda
ARG	Argentina
ARM	Armenia
ABW	Aruba
AP	Asia/Pacific Region
AUS	Australia
AUT	Austria
AZE	Azerbaijan
BHS	Bahamas
BHR	Bahrain
BGD	Bangladesh
BRB	Barbados
BLR	Belarus
BEL	Belgium
BLZ	Belize

Table 72: Sort by Country *(continued)*

BEN	Benin
BMU	Bermuda
BTN	Bhutan
BOL	Bolivia
BIH	Bosnia and Herzegovina
BWA	Botswana
BV	Bouvet Island
BRA	Brazil
IO	British Indian Ocean Territory
BRN	Brunei Darussalam
BGR	Bulgaria
BFA	Burkina Faso
BDI	Burundi
KHM	Cambodia
CMR	Cameroon
CAN	Canada
CPV	Cape Verde
CYM	Cayman Islands
CAF	Central African Republic
TCD	Chad
CHL	Chile
CHN	China
CX	Christmas Island
CC	Cocos (Keeling) Islands
COL	Colombia

Table 72: Sort by Country *(continued)*

COM	Comoros
COG	Congo
COD	Congo, The Democratic Republic of the
COK	Cook Islands
CRI	Costa Rica
CIV	Côte d’Ivoire
HRV	Croatia
CUB	Cuba
CYP	Cyprus
CZE	Czech Republic
DNK	Denmark
DJI	Djibouti
DMA	Dominica
DOM	Dominican Republic
ECU	Ecuador
EGY	Egypt
SLV	El Salvador
GNQ	Equatorial Guinea
ERI	Eritrea
EST	Estonia
ETH	Ethiopia
EU	Europe
FLK	Falkland Islands (Malvinas)
FRO	Faroe Islands
FJI	Fiji

Table 72: Sort by Country *(continued)*

FIN	Finland
FRA	France
FX	France, Metropolitan
GUF	French Guiana
PYF	French Polynesia
TF	French Southern Territories
GAB	Gabon
GMB	Gambia
GEO	Georgia
DEU	Germany
GHA	Ghana
GIB	Gibraltar
GRC	Greece
GRL	Greenland
GRD	Grenada
GLP	Guadeloupe
GUM	Guam
GTM	Guatemala
GGY	Guernsey
GIN	Guinea
GNB	Guinea-Bissau
GUY	Guyana
HTI	Haiti
HM	Heard Island and McDonald Islands
VAT	Holy See (Vatican City State)

Table 72: Sort by Country *(continued)*

HND	Honduras
HKG	Hong Kong
HUN	Hungary
ISL	Iceland
IND	India
IDN	Indonesia
IRN	Iran, Islamic Republic of
IRQ	Iraq
IRL	Ireland
IMN	Isle of Man
ISR	Israel
ITA	Italy
JAM	Jamaica
JPN	Japan
JEY	Jersey
JOR	Jordan
KAZ	Kazakhstan
KEN	Kenya
KIR	Kiribati
PRK	Korea, Democratic People’s Republic of
KOR	Korea, Republic of
KWT	Kuwait
KGZ	Kyrgyzstan
LAO	Lao People’s Democratic Republic
LVA	Latvia

Table 72: Sort by Country *(continued)*

LBN	Lebanon
LSO	Lesotho
LBR	Liberia
LBY	Libyan Arab Jamahiriya
LIE	Liechtenstein
LTU	Lithuania
LUX	Luxembourg
MAC	Macau
MKD	Macedonia
MDG	Madagascar
MWI	Malawi
MYS	Malaysia
MDV	Maldives
MLI	Mali
MLT	Malta
MHL	Marshall Islands
MTQ	Martinique
MRT	Mauritania
MUS	Mauritius
YT	Mayotte
MEX	Mexico
FSM	Micronesia, Federated States of
MDA	Moldova, Republic of
MCO	Monaco
MNG	Mongolia

Table 72: Sort by Country *(continued)*

MNE	Montenegro
MSR	Montserrat
MAR	Morocco
MOZ	Mozambique
MMR	Myanmar
NAM	Namibia
NRU	Nauru
NPL	Nepal
NLD	Netherlands
ANT	Netherlands Antilles
NCL	New Caledonia
NZL	New Zealand
NIC	Nicaragua
NER	Niger
NGA	Nigeria
NIU	Niue
NFK	Norfolk Island
MNP	Northern Mariana Islands
NOR	Norway
OMN	Oman
O1	Other
PAK	Pakistan
PLW	Palau
PSE	Palestinian Territory
PAN	Panama

Table 72: Sort by Country *(continued)*

PNG	Papua New Guinea
PRY	Paraguay
PER	Peru
PHL	Philippines
PCN	Pitcairn Islands
POL	Poland
PRT	Portugal
PRI	Puerto Rico
QAT	Qatar
REU	Reunion
ROU	Romania
RUS	Russian Federation
RWA	Rwanda
SHN	Saint Helena
KNA	Saint Kitts and Nevis
LCA	Saint Lucia
SPM	Saint Pierre and Miquelon
VCT	Saint Vincent and the Grenadines
WSM	Samoa
SMR	San Marino
STP	Sao Tome and Principe
A2	Satellite Provider
SAU	Saudi Arabia
SEN	Senegal
SRB	Serbia

Table 72: Sort by Country *(continued)*

SYC	Seychelles
SLE	Sierra Leone
SGP	Singapore
SVK	Slovakia
SVN	Slovenia
SLB	Solomon Islands
SOM	Somalia
ZAF	South Africa
GS	South Georgia and the South Sandwich Islands
ESP	Spain
LKA	Sri Lanka
SDN	Sudan
SUR	Suriname
SJM	Svalbard and Jan Mayen
SWZ	Swaziland
SWE	Sweden
CHE	Switzerland
SYR	Syrian Arab Republic
TWN	Taiwan
TJK	Tajikistan
TZA	Tanzania, United Republic of
THA	Thailand
TLS	Timor-Leste
TGO	Togo
TKL	Tokelau

Table 72: Sort by Country *(continued)*

TON	Tonga
TTO	Trinidad and Tobago
TUN	Tunisia
TUR	Turkey
TKM	Turkmenistan
TCA	Turks and Caicos Islands
TUV	Tuvalu
UGA	Uganda
UKR	Ukraine
ARE	United Arab Emirates
GBR	United Kingdom
USA	United States
UM	United States Minor Outlying Islands
URY	Uruguay
UZB	Uzbekistan
VUT	Vanuatu
VEN	Venezuela
VNM	Vietnam
VGB	Virgin Islands, British
VIR	Virgin Islands, U.S.
WLF	Wallis and Futuna
ESH	Western Sahara
YEM	Yemen
ZMB	Zambia
ZWE	Zimbabwe

Related Documentation

- Understanding Index Attack Types on page 249

APPENDIX G

Panel and Connector Locations

DDoS Secure Appliance Panel Information

DDoS Secure-1200-Fail-Safe Panels

Figure 1 on page 279 and Figure 2 on page 279 shows the front and back panel of the DDoS Secure-1200-Fail-safe.

Figure 1: DDoS Secure-1200-Fail-Safe Front Panel

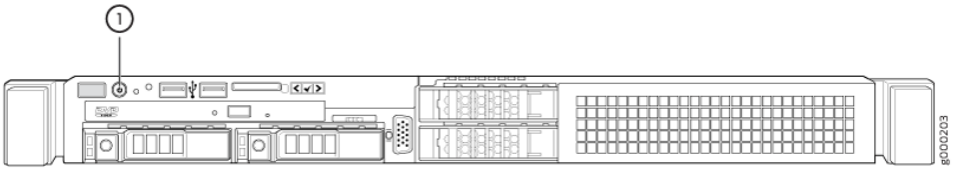


Figure 2: DDoS Secure-1200-Fail-Safe Back Panel

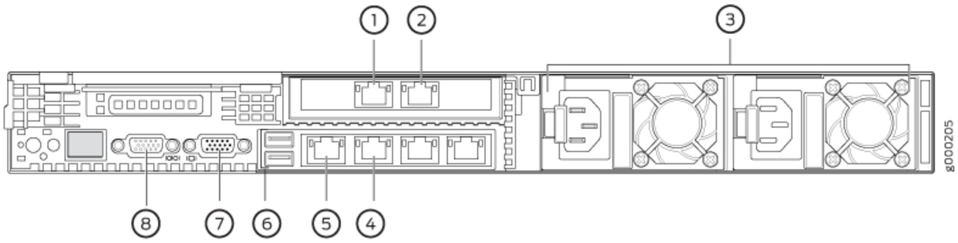


Table 73 on page 279 lists the front and back panel components of the DDoS Secure-1200-Fail-Safe appliance.

Table 73: DDoS Secure 1200-Fail-Safe Callout Details

Callout	Component
Front Panel	
1	Power ON/OFF button
Rear Panel	

Table 73: DDoS Secure 1200-Fail-Safe Callout Details *(continued)*

Callout	Component
1	I-IF (1Gb/10Gb Internet interface)
2	P-I/F (1Gb/10Gb protected interface)
3	Power supply
4	D-IF (Optional 1Gb data share interface)
5	M-I/F+ILO (1Gb management interface and Integrated Lights Out)
6	USB port (Optional)
7	Video (Optional)
8	Serial interface

Related Documentation

- Understanding Index Attack Types on page 249

APPENDIX H

Troubleshooting

Troubleshooting a DDoS Secure Appliance

1. My browser gives an SSL connection error.

   If the DDoS Secure appliance SSL certificate changes for any reason, some PC browsers choke on the previously installed certificate. If so, the old certificate will have to be removed by hand from the Browser Root Certificate cache. It is possible that exiting the browser and reconnecting fixes the situation.

2. How do I recover my lost username and password?

   You are unable to recover the username and password. If Juniper Networks personnel able to access your appliance, they might be able to reset the password. It might be that you have to re-image the system.

3. What does **Init Phase xxx** mean?

   When the appliance starts up, various large data sets have to be initialized. Each phase is the initialization of a different data set.

4. What does **Exit Phase xxx** mean?

   When the appliance closes down, various large data sets have to be cleanly closed down. Each phase is the cleanup of a different data set.

5. Why do I get **Protected IP Table Full** turning to red?

   The appliance is set up to protect a maximum number of protected IP addresses. If this limit is exceeded, then protected IP address table full will turn to red. If your **I-I/F** and **P-I/F** connectors are reversed, the appliance is effectively protecting the Internet from your internal users. Confirm this using the **Protected Information** option. Correct any cabling errors. Review the location of the appliance in your network topology, if the appliance has to protect more than the specified number of protected IP addresses. If cabling arrangements are logically reversed without physical disconnection, the DDoS Secure appliance engine must be restarted to ensure the correct automatic detection of the network topology. It is also possible to swap the interfaces with **Configure Interfaces** option.

Related Documentation

- Understanding Index Attack Types on page 249

APPENDIX I

GUI Branding

Customizing the DDoS Secure Web Interface

You can customize both the GUI initial login landing page and the format/style of pages.

Login Page

To customize the login page:

1. Take a copy of the source of the initial login page, https://a.b.c.d, and save it locally.
2. Name the file customer.tmpl or host_uri-customer.tmpl, where host_uri is the name or IP address that a user uses to access the DDoS Secure appliance.

   The customer.tmpl file:

   - Is preserved across software upgrades.
   - Can include references to external URLs.
   - Can reference existing image files or portal-specific images.
   - Must link to webviewcheck.wsp to enter the DDoS Secure appliance portal.

   For example, If the site is accessed with the URL https://some.host.com, then the search sequence is some.host.com-customer.tmpl, then customer.tmpl, and finally the original login page.

Images/CSS Files

Once you have logged in, you are associated with a portal. Any *.css* file in the */css* directory, or any images in the */images* directory, can be customized to modify the output.

For example, you are logged in to portal CustomerX and are requesting css/center_pane.css. The search order is css/portal-CustomerX-center_pane.css, then css/portal-center_pane.css, and finally css/center_pane.css. The same is true for any images.

Updating Customized Files

To upload the files on a Linux server, you need to collect all the customized files in a directory, and then run the following Linux command to create an update package:

```
echo w.x.y > webscreen- ; tar cvf files.upg webscreen- *customer.tmpl portal*.css portal*.gif
```

where **w.x.y** is the current version of the DDoS Secure appliance (for example: 5.13.1), and then upload files.upg as a DDoS Secure appliance patch.

Removing Customized Files

Run the following command from the CLI to remove any custom files:

```
JS>system clear_custom
```