CHAPTER 10

Configuring DDoS Prevention

This chapter describes how to configure a GSS to prevent Distributed Denial of Service (DDoS) attacks. It contains the following major sections:

Each GSS supports a comprehensive set of **show** CLI commands to display DDoS statistics for the GSS device. In addition, the primary GSSM GUI displays DDoS statistics for the GSS network. See Chapter 13, Displaying GSS Global Server Load-Balancing Statistics, for details about viewing DDoS statistics.

Logging in to the CLI and Enabling Privileged EXEC Mode

Note To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

2. Specify your GSS administrative username and password to log in to the GSSM. The CLI prompt appears.

```
gssm1.example.com>
```

3. At the CLI prompt, enable privileged EXEC mode as follows:

```
gssm1.example.com> enable
gssm1.example.com#
```

If you are accessing the GSS remotely using Telnet or SSH, the CLI prompts you for the enable password. The default password is default. For more information about the enable password and configuring a new password, see the *Cisco Global Site Selector Getting Started Guide*.

Enabling or Disabling DDoS Detection and Mitigation

You configure DDoS on a per-GSS basis using the CLI only. Enable the DDoS detection and mitigation module in the GSS by entering the **enable** command in ddos configuration mode. The **no** form of this command disables DDoS detection and mitigation.

The syntax of this command is as follows:

enable

Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

To display the current operating state of the DDoS detection and mitigation module, use either the **show status** command in the ddos configuration mode or the **show ddos status** command in the privileged EXEC mode.

Note When you enable DDoS detection and mitigation, the first request of the Boomerang proximity method will not work as expected. All subsequent requests will operate correctly until a D-proxy timeout occurs.

As a workaround, you can specify the D-proxy IP address as trusted on the GSS- even for a first request. For more information, see the "Configuring Trusted or Spoofed D-proxies" section.

For example:

```
gssm1.example.com> enable
gssm1.example.com# config
gssm1.example.com(config)# ddos
gssm1.example.com(config-ddos)# enable
```

Modifying or Restoring Rate Limits

The GSS enforces a limit on the number of DNS packets per minute for each individual D-proxy, an overall global rate limit, and a rate limit (unknown rate-limit) that limits the number of anti-spoofing tests to be performed by the GSS in a minute. The GSS enforces rate limits for DNS traffic only; it does not enforce limits for all traffic. You can configure the rate limit for DNS packets from a particular D-proxy only by providing the IP address.

Note The rate-limit is applied to requests entering on port 53 and responses entering on port 5301.

The initial number of requests per minute for each D-proxy is 60. This initial limit is a default value that you can adjust during peacetime learning (see Configuring Peacetime Learning), or override when you configure either a D-proxy or a group of D-proxies. Once this limit is exceeded, DNS packets are dropped.

Note A time window exists when specifying a rate limit. Thus, if the rate-limit for a particular D-proxy is set to 40, the rate limit will force the GSS to drop packets if the limit is exceeded within 60 seconds from the beginning of the first request.

The GSS also enforces a limit on the number of new (unknown) D-proxies for which it will perform an anti-spoofing test in one minute. Once this limit is reached, the GSS drops DNS packets from new sources during that minute. By default, the GSS performs spoof tests for 1000 new D-proxies per minute. You can change this limit by configuring the unknown rate limit.

You can configure or modify the rate-limit for a particular D-proxy, specify a global rate-limit, or configure the number of anti-spoofing tests to be performed by the GSS in a minute by using the **rate-limit** command in ddos configuration mode. This command overrides the default rate limit values. The **no** form of this command turns off rate limits.

The syntax of this command is as follows:

rate-limit {*ipaddress* | **global** | **unknown**} *rate-limit*

The keywords and arguments for this command are as follows:

- *ipaddress*—IP address of the D-proxy. The default value (per minute) for each D-proxy is 60.
- **global**—Specifies the total number of packets per minute from all D-proxies allowed on the GSS. The default value (per minute) is 90,000.
- **unknown**—Specifies the number new D-proxies for which the GSS will perform an anti-spoofing test in one minute. By default, the GSS performs spoof tests for 1000 new D-proxies per minute. Once this limit is reached, the GSS drops DNS packets from new sources during that minute. The spoof test marks the D-proxy as trusted or spoofed. A marked D-proxy remains as marked for one hour.

Note By configuring the unknown rate-limit, you enable the GSS to handle random spoofed attacks in which there is a flood of unknown D-proxies. When the GSS is under random spoofed attack, new valid D-proxies compete against spoofed D-proxies. In such cases, if the total number of new D-proxies (spoofed and valid) exceeds the unknown rate limit, some valid D-proxies are dropped. However, service to known D-proxies is not affected.

- *rate-limit* —Maximum number of DNS packets the GSS will receive per minute. You must enter absolute values here, such as 1, 2, and 3. You cannot enter fractional values, such as 1.1, 2.2, and 3.3. For the lower limit of the range, you cannot enter a value that is less than 0.

After a limit is reached for a particular category, the GSS does not respond to more of those types of requests for one minute. The **ddos restore-default** command restores the rate limit database values to the default values.

For example, enter:

```
gssm1.example.com(config-ddos)# rate-limit global 10000
gssm1.example.com(config-ddos)# rate-limit unknown 100
gssm1.example.com(config-ddos)# rate-limit 10.1.1.1 500
gssm1.example.com(config-ddos)#
```

To view the applied rate limit and the number of drops, use the **show ddos rate-limit** command.

Disabling the Anti-Spoofing Function

The DDoS function performs anti-spoofing (AS) by redirecting a DNS request over TCP. The DDoS AS function is enabled by default. You can disable AS to allow the DDoS function to provide protection through rate limiting, even when TCP traffic cannot reach the GSS.

You can disable the AS function by using the **ddos disable-as** configuration command. When you disable anti-spoofing, the unknown rate limit is also disabled; however, the global rate limit and the individual rate limit per D-proxy will work as expected. To enable AS, use the **no** form of the command.

When you disable AS, the DDoS function performs as follows:

- Ignores the configured “Unknown Rate Limit.”
- Does not trigger any new AS checks.
- Does not allow spoofed packet drops or AS ongoing packet drops.
- Does not support spoofed or trusted D-proxy configuration from the DDoS CLI.
- Produces the following message when you enter the **show ddos dproxy** CLI command:

```
gss1.example.com# show ddos-dproxy
Anti-Spoofing is turned off currently. DDoS anti-spoofing values cannot be shown.
```

To disable AS on the GSS, enter:

```
gss1.example.com(config)# ddos disable-as
```

To view the current operating state of the AS function, use the **show ddos-config | grep disable-as** command. If the AS function is enabled, the CLI displays nothing. If the AS function is disabled, the operating state displays as shown in the following example:

```
gss1.example.com(config)# show ddos-config | grep disable-as
ddos
    disable-as
```

Setting a Scaling Factor

The final rate limits per D-proxy are determined by multiplying the rate-limits learned during peacetime with a scaling factor. You can configure this value by using the **scaling-factor** command in ddos configuration mode. The **no** form of this command turns off the scaling factor for rate limits.

The syntax of this CLI command is as follows:

scaling-factor d-proxy *value*

The keywords and arguments for this command are as follows:

- **d-proxy**—Specifies the D-proxy scaling factor.
- *value*—Tolerance scaling factor for rate limiting. You enter the value as a percentage of the rate limit. The default value here is 100.

To change the current rate limit of 10000 to 5000 or 50 percent of its current value, enter:

```
gssm1.example.com(config-ddos)# scaling-factor d-proxy 50
```

To change that rate limit to 15000 or 150 percent of its current value, enter:

```
gssm1.example.com(config-ddos)# scaling-factor d-proxy 150
```

Configuring Trusted or Spoofed D-proxies

You can manually configure a D-proxy as either trusted or spoofed by using the **dproxy** command in ddos configuration mode.

The syntax of this command is as follows:

dproxy {**spoofed** *ipaddress* | **trusted** *ipaddress* }

The keywords and arguments for this command are as follows:

- **spoofed**—Specifies the D-proxy as spoofed.
- **trusted**—Specifies the D-proxy as trusted.
- *ipaddress*—IP address of the trusted or spoofed D-proxy.

No anti-spoofing checks are done for entries that you mark as trusted or spoofed. If you configure a D-proxy as trusted, the GSS does not perform the anti-spoofing test on DNS packets from that IP address. If you configure a D-proxy as spoofed, DNS packets from that IP address will be dropped. These commands will override the learned and default values.

Note The entries that you add using the CLI will not time out. You can remove these entries only by entering the **no dproxy** command.

For example, enter:

```
gssm1.example.com(config-ddos)# dproxy trusted 10.1.1.1
gssm1.example.com(config-ddos)#
```

To view the DDoS configuration, use the **show ddos-config** command.

Enabling or Disabling Mitigation Rule Checks

You can enable mitigation rule checks in the GSS by using the **mitigation-rule** command in ddos configuration mode. The **no** form of this command disables rule checks.

Note By default, mitigation rule checks are enabled.

The syntax of this command is as follows:

mitigation-rule {**response** | **request**} **enable**

The keywords and arguments for this command are as follows:

- **response**—Enables or disables the following mitigation rules for DNS responses:
  - DNS response packets are dropped if they come from a source port other than 53.
  - DNS response packets are dropped if they have a destination port of 53.
- **request**—Enables or disables the mitigation rules for DNS requests in which DNS request packets are dropped if they have a source port neither equal to 53 nor greater the 1024.

For example, enter:

```
gssm1.example.com(config-ddos)# mitigation-rule response enable
gssm1.example.com(config-ddos)#
```

Configuring a Global Domain Name

You can configure the GSS to process requests for only a particular domain. If the GSS receives requests for domains outside the configured domain name, the requests are dropped. You configure a global domain name by using the **global-domain** command in ddos configuration mode.

The syntax of this command is as follows:

global-domain *domain-name*

The *domain-name* argument *s*pecifies the name of the global domain.

The **global-domain** command requires an exact match, so if you enter *.com as a *domain-name*, it does not specify that all domains that are not .com are blocked. When you configure a global domain, the configuration applies to its subdomains also.

The global domain check applies to UDP queries only. You may configure only one global domain at a time. Use this command when the GSS is expected to service queries for only one domain (including its subdomains).

For example, enter:

```
gssm1.example.com(config-ddos)# global-domain cisco.com
gssm1.example.com(config-ddos)#
```

Note If a query contains multiple questions, the request is dropped even if one of the questions fails the domain match.

Configuring Maximum Entries in the DDoS Database

You can configure the maximum number of entries stored in the DDoS database by using the **max-database-entries** command in ddos configuration mode.

The syntax of this command is as follows:

max-database-entries *number*

The *number* argument *s*pecifies the maximum number of entries you wish to store in the GSS database. The range here is from 65536 to 1048576, with a default value of 65536. You can increase or decrease this number to adjust the GSS device.

For example, enter:

```
gssm1.example.com(config-ddos)# max-database-entries 1037300
This command will clear the current DDoS database and create a new database with support
for 1037300 entries.
This command will take effect only after the next gss stop and start.
Do you want to continue? (y/n):y
```

Note You should use **max-database-entries** only if you wish to clear your current DDoS database and reallocate more or less memory for the DDoS module. After entering the command and executing a gss stop, start, or reload, check the DDoS module status by entering **show ddos status**.

If the command fails and the "Error opening device file" message appears, check the syslog-messages.log to determine if a memory allocation failure has occurred. If so, the syslog-messages.log reports the following log message: "Unable to allocate sufficient memory for DDoS kernel module. Module insertion failed."In such cases, you should run **max-database-entries** once more to set a lower value, ignore any error messages that appear, and reboot the GSS.

Executing a Saved DDos Configuration File

You can execute a saved DDoS configuration file by using the **script play-config** command in DDoS configuration mode.

The syntax of this command is as follows:

script play-config *filename*

The *filename* argument specifies the filename of the saved DDoS configuration that you want to execute.

For example, enter:

```
gssm1.example.com (config-ddos)# script play-config ddos_config.txt
```

Configuring Peacetime Learning

Run the peacetime learning module on the GSS when you do not want to use the default per-D-proxy rate limit (60 DNS packets per minute), but rather, you want to learn the characteristics of the traffic flow between each D-proxy and the GSS over a period of time and apply the learned rate limits. By running the peacetime learning command for a period of time, you obtain a sampling of typical traffic behaviors.

The GSS acquires the baseline or traffic pattern of the specific zone and populates the DDoS rate-limiting database with threshold rate limits that you can then apply to the GSS by using the CLI commands.

You can use peacetime rate limits to modify default or configured rate-limit values. The applied peacetime rate limits do not affect the **unknown** or **global** rate limit configurations.

This section contains the following topics:

Starting Peacetime Learning

You can start the peacetime learning process by using the **ddos peacetime start** command in privileged EXEC mode. This command incrementally updates the values in the peacetime database. To ensure that the database is empty prior to beginning the peacetime learning process, enter the **ddos peacetime database erase** command before using the **ddos peacetime start** command (see the "Erasing Peacetime Learning" section).

The syntax of this command is as follows:

ddos peacetime start

For example, enter:

```
gssm1.example.com# ddos peacetime start
gssm1.example.com#
```

Stopping Peacetime Learning

You can stop peacetime learning by using the **ddos peacetime stop** command in privileged EXEC mode.

The syntax of this command is as follows:

ddos peacetime stop

For example, enter:

```
gssm1.example.com# ddos peacetime stop
gssm1.example.com#
```

Saving Peacetime Learning

You can save peacetime learning to a file on disk by using the **ddos peacetime save** command in privileged EXEC mode.

The syntax of this command is as follows:

ddos peacetime save *filename*

The *filename* argument *s*pecifies the name of the file on disk to which you wish to save peacetime learning.

For example, enter:

```
gssm1.example.com# ddos peacetime save
gssm1.example.com#
```

Showing Peacetime Learning

You can show the values learned during the peacetime learning process, or the peacetime learning status by using the **ddos peacetime show** command in privileged EXEC mode.

The syntax of this command is as follows:

ddos peacetime show [*filename* | **status**]

The keywords and arguments for this command are as follows:

- *filename*—Filename of the peacetime learning process for which you want to display values.
- **status**—Shows the current peacetime learning status.

For example, enter:

```
gssm1.example.com# ddos peacetime show status
DDoS Peacetime Learning is not running.
```

Erasing Peacetime Learning

You can erase peacetime learning by using the **ddos peacetime database erase** command in privileged EXEC mode.

The syntax of this command is as follows:

ddos peacetime database erase

For example, enter:

```
gssm1.example.com# ddos peacetime database erase
```

```
gssm1.example.com#
```

Setting the Location for the Peacetime File

You can set the location or file that the peacetime file uses in a **ddos peacetime apply** operation by using the **peacetime database** command in ddos configuration mode. The peacetime database location is specified when you use the **peacetime database** command

The syntax of this command is as follows:

peacetime database *file*

The *file argument s*pecifies the peacetime file to use.

Note If you do not configure a location for the peacetime file, or if you enter the **no peacetime database** command, the result is that the peacetime database is used from system memory.

For example, enter:

```
gssm1.example.com(config-ddos)# peacetime database samplefile
gssm1.example.com(config-ddos)#
```

Applying Peacetime Values

You can apply values learned during the peacetime learning process to the rate-limit database by using the **ddos peacetime apply** command in privileged EXEC mode. This command updates the rate-limit database with the peacetime learned values.

The peacetime database location is specified in the **peacetime database** command. If you do not specify this command, the in-memory database is used instead.

The syntax of this command is as follows:

ddos peacetime apply {**increment** | **overwrite**}

The keywords and arguments are as follows:

- **increment**—Specifies that you want to apply the peacetime learned values incrementally to the database.
- **overwrite**—Specifies that you want to restore all the values in the rate-limit database to their defaults and then update them with the values learned during peacetime.

For example, enter:

```
gssm1.example.com# ddos peacetime apply increment
gssm1.example.com#
```

Managing Your DDoS Configuration

Two commands are available that allow you to manage your DDoS configuration. This section describes the following topics:

Copying a DDoS Configuration to Disk

You copy the DDoS configuration to disk by entering the **copy ddos-config** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

copy ddos-config disk *filename*

The **disk** *filename* keyword and argument indicate that you want to copy the configuration to disk and store it under the specified file name.

For example, enter:

```
gssm1.example.com# copy ddos-config disk ddos_config.txt
gssm1.example.com#
```

Clearing a DDoS Configuration

You clear a DDoS configuration by entering the **clear ddos-config** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

clear ddos-config

For example, enter:

```
gssm1.example.com# clear ddos-config
gssm1.example.com#
```

Restoring DDoS Defaults

You restore the default values in the rate-limit database by entering the **ddos restore-defaults** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

ddos restore-defaults *ipaddress*

The *ipaddress* argument specifies the D-proxy IP address and indicates that you wish to restore the rate limit of the designated D-proxy to the default rate and the state to Unknown.

For example, enter:

```
gssm1.example.com# ddos restore-defaults 1.1.1.2
```

Where to Go Next

Chapter 11, Creating and Playing GSLB Configuration Files, describes how to create, modify, and play (execute) GSLB configuration files.