

# DDoS Module Configuration Mode Commands

This section describes the commands in the Distributed Denial of Service (DDoS) module configuration mode. The DDoS configuration mode commands allow you to configure DDoS detection and mitigation functions on the GSS.

To access the DDoS configuration mode, use the **ddos** command in global configuration mode. The CLI prompt then changes to the DDoS module configuration mode as follows:

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

```
ddos [disable-as | dproxy {spoofed ipaddress | trusted ipaddress} | enable
| global-domain domain-name |
max-database-entries number | mitigation-rule {response | request}
enable | peacetime database file | rate-limit {ipaddress | global |
unknown} rate-limit | scaling-factor d-proxy value | script play-config
filename]
```

<b>disable-as</b>	See the <a href="#">(config-ddos) disable-as</a> command for a detailed syntax description.
<b>dproxy</b> [ <b>spoofed</b> <i>ipaddress</i>   <b>trusted</b> <i>ipaddress</i> ]	See the <a href="#">(config-ddos) dproxy</a> command for a detailed syntax description.
<b>enable</b>	See the <a href="#">(config-ddos) enable</a> command for a detailed syntax description.
<b>global-domain</b> <i>domain-name</i>	See the <a href="#">(config-ddos) global-domain</a> command for a detailed syntax description.
<b>max-database-entries</b> <i>number</i>	See the <a href="#">(config-ddos) max-database-entries</a> command for a detailed syntax description.
<b>mitigation-rule</b> { <b>response</b>   <b>request</b> } <b>enable</b>	See the <a href="#">(config-ddos) mitigation-rule</a> command for a detailed syntax description.
<b>peacetime database</b> <i>file</i>	See the <a href="#">(config-ddos) peacetime database</a> command for a detailed syntax description.
<b>rate-limit</b> { <i>ipaddress</i>   <b>global</b>   <b>unknown</b> } <i>rate-limit</i>	See the <a href="#">(config-ddos) rate-limit</a> command for a detailed syntax description.

---

<b>scaling-factor d-proxy</b> <i>value</i>	See the <a href="#">(config-ddos) scaling-factor</a> command for a detailed syntax description.
<b>script play-config</b> <i>filename</i>	See the <a href="#">(config-ddos) script play-config</a> command for a detailed syntax description.

---

## (config-ddos) disable-as

To disable anti-spoofing (AS), use the **disable-as** configuration command. When you disable AS, the unknown rate limit is also disabled; however, the individual rate limit per D-proxy will work as expected. To enable AS, use the **no** form of the command.

**disable-as**

**no disable-as**

---

### Syntax Description

This command has no keywords or arguments.

---

### Command Modes

DDoS configuration.

---

### Usage Guidelines

The DDoS function performs AS by redirecting a DNS request over TCP. You can disable AS to allow the DDoS function to provide protection through rate limiting, even when TCP traffic cannot reach the GSS.

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 view the current operating state of the AS function, use the following command:

```
show ddos-config | grep disable-as
```

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
```

---

### Examples

The following example shows how to disable AS on the GSS:

```
gssm1.example.com(config-ddos)# disable-as  
gssm1.example.com(config-ddos)#
```

---

### Related Commands

- [\(config-ddos\) dproxy](#)
- [\(config-ddos\) enable](#)
- [\(config-ddos\) global-domain](#)
- [\(config-ddos\) max-database-entries](#)
- [\(config-ddos\) mitigation-rule](#)
- [\(config-ddos\) peacetime database](#)
- [\(config-ddos\) rate-limit](#)
- [\(config-ddos\) scaling-factor](#)
- [\(config-ddos\) script play-config](#)

## (config-ddos) dproxy

To configure trusted or spoofed D-proxies, use the **dproxy** command. To remove entries added using the CLI since these entries will not time out, use the **no** form of this command.

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

**no dproxy** {spoofed *ipaddress* | trusted *ipaddress*}

### Syntax Description

<b>spoofed</b>	Sets the D-proxy as spoofed.
<b>trusted</b>	Sets the D-proxy to trusted.
<i>ipaddress</i>	IP address of the trusted or spoofed D-proxy.

### Command Modes

DDoS configuration.

### Usage Guidelines

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.

### Examples

The following example shows how to configure trusted or spoofed D-proxies:

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

### Related Commands

[\(config-ddos\) disable-as](#)  
[\(config-ddos\) enable](#)  
[\(config-ddos\) global-domain](#)  
[\(config-ddos\) max-database-entries](#)  
[\(config-ddos\) mitigation-rule](#)

**(config-ddos) peacetime database**

**(config-ddos) rate-limit**

**(config-ddos) scaling-factor**

**(config-ddos) script play-config**

## (config-ddos) enable

To enable the Distributed Denial of Service (DDoS) detection and mitigation module in the GSS, use the **enable** command in DDoS configuration mode. To disable DDoS detection in the GSS, use the **no** form of this command.

**enable**

**no enable**

---

### Syntax Description

This command has no keywords or arguments.

---

### Command Modes

DDoS configuration

---

### Examples

The following example shows how to enable DDoS detection and mitigation in the GSS:

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

The following example shows how to disable DDoS detection and mitigation in the GSS:

```
gssm1.example.com(config)# ddos  
gssm1.example.com(config-ddos)# no enable  
gssm1.example.com(config-ddos)# exit  
gssm1.example.com(config)#
```

---

### Related Commands

[\(config-ddos\) disable-as](#)

[\(config-ddos\) dproxy](#)

[\(config-ddos\) global-domain](#)

[\(config-ddos\) max-database-entries](#)

[\(config-ddos\) mitigation-rule](#)

[\(config-ddos\) peacetime database](#)

**(config-ddos) rate-limit**

**(config-ddos) scaling-factor**

**(config-ddos) script play-config**

# (config-ddos) global-domain

To configure a global domain name, use the **global-domain** command.

**global-domain** *domain-name*

---

## Syntax Description

*domain-name*

Name of the global domain. The **global-domain** command requires an exact match. If you enter \*.com as a *domain-name*, it does not specify that all domains that are not .com are blocked.

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

---

---

## Command Modes

DDoS configuration

---

## Usage Guidelines

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.

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).

---

## Examples

The following example shows how to configure a global domain name:

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

---

## Related Commands

[\(config-ddos\) disable-as](#)

[\(config-ddos\) dproxy](#)

[\(config-ddos\) enable](#)

**(config-ddos) max-database-entries**

**(config-ddos) mitigation-rule**

**(config-ddos) peacetime database**

**(config-ddos) rate-limit**

**(config-ddos) scaling-factor**

**(config-ddos) script play-config**

## (config-ddos) max-database-entries

To configure the maximum number of entries stored in the Distributed Denial of Service (DDoS) database, use the **max-database-entries** command. To disable the configuration of the maximum number of database entries, use the **no** form of this command.

**max-database-entries** *number*

**no max-database-entries** *number*

---

### Syntax Description

---

<i>number</i>	Maximum number of entries that you want to store in the GSS database from 65536 to 1048576 with a default of 65536. You can increase or decrease this number.
---------------	---

---

---

### Command Modes

DDoS configuration

---

### Usage Guidelines

Use the **max-database-entries** command only if you want to clear your current DDoS database and reallocate more or less memory for the DDoS module. After entering this command and executing a `gss stop`, `gss start`, or `gss 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.

---

### Examples

The following example shows how to configure the maximum number of entries stored in the DDoS database:

```
gssm1.example.com(config-ddos)# max-database-entries 1037300
```

**DDoS Module Configuration Mode Commands**

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**

**Related Commands**

**(config-ddos) disable-as**  
**(config-ddos) dproxy**  
**(config-ddos) enable**  
**(config-ddos) mitigation-rule**  
**(config-ddos) peacetime database**  
**(config-ddos) rate-limit**  
**(config-ddos) scaling-factor**  
**(config-ddos) script play-config**

## (config-ddos) mitigation-rule

To enable mitigation rule checks in the GSS, use the **mitigation-rule** command. To disable mitigation rule checks, use the **no** form of this command. By default, mitigation rule checks are enabled.

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

**no mitigation-rule** {response | request} enable

### Syntax Description

<b>response</b>	Enables or disables the following mitigation rules for Domain Name System (DNS) responses: <ul style="list-style-type: none"> <li>DNS response packets are dropped if they come from a source port other than 53.</li> <li>DNS response packets are dropped if they have a destination port of 53.</li> </ul>
<b>request</b>	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.

### Command Modes

DDoS configuration

### Examples

The following example shows how to enable mitigation rule checks in the GSS:

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

### Related Commands

(config-ddos) disable-as  
 (config-ddos) dproxy  
 (config-ddos) enable  
 (config-ddos) global-domain

**(config-ddos) max-database-entries**

**(config-ddos) peacetime database**

**(config-ddos) rate-limit**

**(config-ddos) scaling-factor**

**(config-ddos) script play-config**

## (config-ddos) peacetime database

To set the location or file that the peacetime file uses in a **ddos peacetime apply** operation, use the **peacetime database** command. To not configure this command or cause the peacetime database in memory to be used, use the **no** form of this command.

**peacetime database** *file*

**no peacetime database** *file*

---

### Syntax Description

---

*file* Peacetime file to be used.

---

---

### Command Modes

DDoS configuration

---

### Examples

The following example shows how to set the location or file that the peacetime file uses in a **ddos peacetime apply** operation:

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

---

### Related Commands

[ddos peacetime apply](#)  
[\(config-ddos\) disable-as](#)  
[\(config-ddos\) dproxy](#)  
[\(config-ddos\) enable](#)  
[\(config-ddos\) global-domain](#)  
[\(config-ddos\) max-database-entries](#)  
[\(config-ddos\) mitigation-rule](#)  
[\(config-ddos\) rate-limit](#)  
[\(config-ddos\) scaling-factor](#)  
[\(config-ddos\) script play-config](#)

## (config-ddos) rate-limit

To configure or modify the rate limit for a particular D-proxy, to set a global rate limit, or to limit the number of anti-spoofing tests to be performed by the GSS in a minute, use the **rate-limit** command. To turn off the rate limits, use the **no** form of this command.

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

```
no rate-limit { ipaddress | global | unknown } rate-limit
```

### Syntax Description

<i>ipaddress</i>	IP address of the D-proxy. The default (per minute) for each D-proxy is 60.
<b>global</b>	Specifies the global rate limit on the GSS. The default per minute is 90,000.
<b>unknown</b>	Specifies the number of new (unknown) D-proxies for which the GSS will perform an anti-spoofing test in one minute.
<i>rate-limit</i>	Maximum number of DNS requests that the GSS can receive from a D-proxy per minute.
	<b>Note</b> You must enter absolute values, 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.

### Command Modes

DDoS configuration

### Usage Guidelines

A time window exists when specifying a rate limit. If the rate limit for a particular D-proxy is set to 40, the rate limit will drop DNS packets if the limit is exceeded within 1 minute (60 seconds) from the beginning of the first request.

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. If the total number of new D-proxies (spoofed and valid) exceeds the unknown rate limit, some valid D-proxies are dropped. However, the service to known D-proxies is not affected.

Once the unknown 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.

---

### Examples

The following example shows how to set a global rate limit:

```
gssm1.example.com(config-ddos)# rate-limit 10.1.1.1 global 1000  
gssm1.example.com(config-ddos)#
```

---

### Related Commands

([config-ddos](#)) [disable-as](#)  
([config-ddos](#)) [dproxy](#)  
([config-ddos](#)) [enable](#)  
([config-ddos](#)) [global-domain](#)  
([config-ddos](#)) [max-database-entries](#)  
([config-ddos](#)) [mitigation-rule](#)  
([config-ddos](#)) [peacetime database](#)  
([config-ddos](#)) [scaling-factor](#)  
([config-ddos](#)) [script play-config](#)

## (config-ddos) scaling-factor

To configure the final rate limits per D-proxy and for all D-proxies, use the **scaling-factor** command. To turn off the scaling factor for rate limits, use the **no** form of this command.

**scaling-factor d-proxy** *value*

**no scaling-factor dproxy** *value*

Syntax	Description
<b>d-proxy</b>	Specifies the D-proxy scaling factor.
<i>value</i>	Tolerance scaling factor for rate limiting.
<b>Note</b>	You enter the value as a percentage of the rate limit. The default value is 100.

**Command Modes** DDoS configuration

**Usage Guidelines** The final rate limits per D-proxy are determined by multiplying the rate limits learned during peacetime with a scaling factor.

**Examples** The following example shows how to change the current rate limit of 10000 to 5000 or 50 percent of its current value:

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

The following example shows how to change that rate limit to 15000 or 150 percent of its current value:

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

**Related Commands** [\(config-ddos\) disable-as](#)  
[\(config-ddos\) dproxy](#)

(config-ddos) enable  
(config-ddos) global-domain  
(config-ddos) max-database-entries  
(config-ddos) mitigation-rule  
(config-ddos) peacetime database  
(config-ddos) rate-limit  
(config-ddos) script play-config

## (config-ddos) script play-config

To execute a saved Distributed Denial of Service (DDoS) configuration file, use the **script play-config** command in DDoS configuration mode. To disable DDoS configuration file execution, use the **no** form of this command.

**script play-config** *filename*

**no script play-config** *filename*

<b>Syntax Description</b>	<i>filename</i>	Filename of the saved DDoS configuration that you want to execute.
---------------------------	-----------------	--

<b>Command Modes</b>	DDoS configuration
----------------------	--------------------

<b>Examples</b>	The following example shows how to execute the saved <i>ddos_config.txt</i> configuration file:
-----------------	---

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

<b>Related Commands</b>	<p><a href="#">(config-ddos) disable-as</a></p> <p><a href="#">(config-ddos) dproxy</a></p> <p><a href="#">(config-ddos) enable</a></p> <p><a href="#">(config-ddos) global-domain</a></p> <p><a href="#">(config-ddos) max-database-entries</a></p> <p><a href="#">(config-ddos) mitigation-rule</a></p> <p><a href="#">(config-ddos) peacetime database</a></p> <p><a href="#">(config-ddos) rate-limit</a></p> <p><a href="#">(config-ddos) scaling-factor</a></p>
-------------------------	---

## (config-ddos) show

To display Distributed Denial of Service (DDoS) parameters, use the **show** command and its variations.

```
show [attacks | dproxy [ipaddress | trusted | spoofed] | failed-dns
      [failed-domains | global-domain-rules | gslb-rules] | rate-limit
      [ipaddress | global] | ddos-config | statistics [attacks | global] | status]
```

<b>attacks</b>	See the <a href="#">show attacks</a> command for a detailed syntax description.
<b>dproxy</b> [ <i>ipaddress</i>   <b>trusted</b>   <b>spoofed</b> ]	See the <a href="#">show dproxy</a> command for a detailed syntax description.
<b>failed-dns</b> { <b>failed-domains</b>   <b>global-domain-rules</b>   <b>gslb-rules</b> }	See the <a href="#">show failed-dns</a> command for a detailed syntax description.
<b>rate-limit</b> [ <i>ipaddress</i>   <b>global</b> ]	See the <a href="#">show rate-limit</a> command for a detailed syntax description.
<b>ddos-config</b>	See the <a href="#">show ddos-config</a> command for a detailed syntax description.
<b>statistics</b> [ <b>attacks</b>   <b>global</b> ]	See the <a href="#">show statistics</a> command for a detailed syntax description.
<b>status</b>	See the <a href="#">show status</a> command for a detailed syntax description.

## show attacks

To display Domain Name System (DNS) attacks detected by the GSS, use the **show ddos attacks** command.

**show attacks**

---

### Syntax Description

This command has no keywords or arguments.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

For information about the fields in the **show attacks** command output, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

---

### Related Commands

[show dproxy](#)  
[show failed-dns](#)  
[show rate-limit](#)  
[show ddos-config](#)  
[show statistics](#)  
[show status](#)

## show dproxy

To show spoofed and nonspoofed D-proxies on the GSS, use the **show dproxy** command.

```
show dproxy [ipaddress | trusted | spoofed]
```

<b>Syntax Description</b>	<i>ipaddress</i>	(Optional) D-proxy IP address.
	<b>trusted</b>	(Optional) Specifies the trusted D-proxies.
	<b>spoofed</b>	(Optional) Specifies the spoofed D-proxies.

**Command Modes** Privileged EXEC

**Usage Guidelines** For information about the fields in the **show dproxy** command output, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

**Related Commands**

- [show attacks](#)
- [show failed-dns](#)
- [show rate-limit](#)
- [show ddos-config](#)
- [show statistics](#)
- [show status](#)

## show failed-dns

To show the last  $x$  number of domain names that caused the failed Domain Name System (DNS) queries at the GSS or the number of failed DNS queries per D-proxy, use the **show failed-dns** command.

```
show failed-dns { failed-domains | global-domain-rules | gslb-rules }
```

### Syntax Description

<b>failed-domains</b>	Specifies the failed domain names due to a global server load balancing (GSLB)-rule mismatch.  <b>Note</b> Even if Distributed Denial of Service (DDoS) is disabled, you can use this option to list the failed domain names due to the GSLB-rule mismatch. The list is updated even if DDoS is disabled.
<b>global-domain-rules</b>	Specifies the number of failures due to a global domain mismatch.
<b>gslb-rules</b>	Specifies the number of failures due to a GSLB-rule mismatch.

### Command Modes

Privileged EXEC

### Usage Guidelines



#### Note

Failed DNS queries refer to DNS queries for a domain not configured on the GSS.

For information about the fields in the **show failed-dns** command output, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

### Related Commands

[show attacks](#)

[show dproxy](#)

**show rate-limit**

**show ddos-config**

**show statistics**

**show status**

## show rate-limit

To show the rate limits per D-proxy and the number of packets dropped per source, use the **show rate-limit** command.

```
show rate-limit [ipaddress | global | unknown]
```

Syntax Description		
	<i>ipaddress</i>	(Optional) IP address of the D-proxy.
	<b>global</b>	(Optional) Specifies the global rate limit on the GSS.
	<b>unknown</b>	(Optional) Specifies the unknown D-proxy rate limit.

**Usage Guidelines** For information about the fields in the **show rate-limit** command output, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

**Related Commands**

- [show attacks](#)
- [show dproxy](#)
- [show failed-dns](#)
- [show ddos-config](#)
- [show statistics](#)
- [show status](#)

## show ddos-config

To display the contents of the Distributed Denial of Service (DDoS) running configuration file, use the **show ddos-config** command.

**show ddos-config**

---

### Syntax Description

This command has no keywords or arguments.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

For information about the fields in the **show ddos-config** command output, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

---

### Related Commands

[show attacks](#)  
[show dproxy](#)  
[show failed-dns](#)  
[show rate-limit](#)  
[show statistics](#)  
[show status](#)

## show statistics

To display Distributed Denial of Service (DDoS) global or attack statistics, use the **show statistics** command.

**show statistics** [**attacks** | **global**]

### Syntax Description

<b>attacks</b>	(Optional) Displays DDoS attack statistics.
<b>global</b>	(Optional) Displays DDoS global statistics.

### Command Modes

Privileged EXEC

### Usage Guidelines

For information about the fields in the **show statistics** command output, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

### Related Commands

[show attacks](#)  
[show dproxy](#)  
[show failed-dns](#)  
[show rate-limit](#)  
[show ddos-config](#)  
[show status](#)

## show status

To display the status of the Distributed Denial of Service (DDoS) detection and mitigation module on the GSS, use the **show status** command.

**show status**

---

### Syntax Description

This command has no keywords or arguments.

---

### Command Modes

Privileged EXEC

---

### Usage Guidelines

For information about the fields in the **show status** command output, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

---

### Related Commands

[show attacks](#)  
[show dproxy](#)  
[show failed-dns](#)  
[show rate-limit](#)  
[show ddos-config](#)

■ DDoS Module Configuration Mode Commands