Configuring Login Block

Information About Login Enhancements-Login Block

Login Enhancements-Login Block Overview

The Login Enhancements (Login Block) feature allows users to enhance the security of a device by configuring options to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected.

The login block and login delay options introduced by this feature can be configured for Telnet or SSH virtual connections. By enabling this feature, you can slow down “dictionary attacks” by enforcing a “quiet period” if multiple failed connection attempts are detected, thereby protecting the routing device from a type of denial-of-service attack.

Protecting Against Denial of Service and Dictionary Login Attacks

Connecting to a device for the purposes of administering (managing) the device, at either the User or Executive level, is most frequently performed using Telnet or SSH (secure shell) from a remote console (such as a PC). SSH provides a more secure connection option because communication traffic between the user’s device and the managed device are encrypted. The Login Block capability, when enabled, applies to both Telnet connections and SSH connections. Beginning in Release versions 12.3(33)SRB2, 12.2(33)SXH2, and 12.4(15)T1, the Login Block capability also applies to HTTP connections.”

The automated activation and logging of the Login Block and Quiet Period capabilities introduced by this feature are designed to further enhance the security of your devices by specifically addressing two well known methods that individuals use to attempt to disrupt or compromise network devices.

If the connection address of a device is discovered and is reachable, a malicious user may attempt to interfere with the normal operations of the device by flooding it with connection requests. This type of attack is referred to as an attempted Denial-of-Service, because it is possible that the device may become too busy trying to process the repeated login connection attempts to properly handle normal routing services or are not able to provide the normal login service to legitimate system administrators.

The primary intention of a dictionary attack, unlike a typical DoS attack, is to actually gain administrative access to the device. A dictionary attack is an automated process to attempt to login by attempting thousands, or even millions, of username/password combinations. (This type of attack is called a “dictionary attack” because it typically uses, as a start, every word found in a typical dictionary as a possible password.) As scripts or programs are used to attempt this access, the profile for such attempts is typically the same as for DoS attempts; multiple login attempts in a short period of time.

By enabling a detection profile, the device can be configured to react to repeated failed login attempts by refusing further connection request (login blocking). This block can be configured for a period of time, called a “quiet period”. Legitimate connection attempts can still be permitted during a quiet period by configuring an access-list (ACL) with the addresses that you know to be associated with system administrators.

Delays Between Successive Login Attempts

A device can accept virtual connections as fast as they can be processed. Introducing a delay between login attempts helps to protect the device against malicious login connections such as dictionary attacks and DoS attacks. Delays can be enabled in one of the following ways:

- Through the **auto secure** command. If you enable the AutoSecure feature, the default login delay time of one second is automatically enforced.
- Through the **login block-for** command. You must enter this command before issuing the **login delay** command. If you enter only the **login block-for** command, the default login delay time of one second is automatically enforced.
- Through the global configuration mode command, **login delay**, which allows you to specify login delay time to be enforced, in seconds.

Login Shutdown If DoS Attacks Are Suspected

If the configured number of connection attempts fail within a specified time period, the device does not accept any additional connections for a “quiet period.” (Hosts that are permitted by a predefined access-control list [ACL] are excluded from the quiet period.)

The number of failed connection attempts that trigger the quiet period can be specified through the new global configuration mode command **login block-for**. The predefined ACL that is excluded from the quiet period can be specified through the new global configuration mode command **login quiet-mode access-class**.

This functionality is disabled by default, and it is not enabled if AutoSecure if enabled.

How to Configure Login Enhancements-Login Block

Configuring Login Parameters

Use this task to configure your device for login parameters that help detect suspected DoS attacks and slow down dictionary attacks.

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of one second
- All login attempts made through Telnet or SSH are denied during the quiet period; that is, no ACLs are exempt from the login period until the **login quiet-mode access-class** command is issued.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**login block-for** *seconds* **attempts** *tries* **within** *seconds* **Example:** `Device(config)# login block-for 100 attempts 2 within 100`	Configures your device for login parameters that help provide DoS detection. **Note** This command must be issued before any other login command can be used.

Step 4	**login quiet-mode access-class** {*acl-name* | *acl-number*}
	Example:
	`Device(config)# login quiet-mode access-class myacl`
		(Optional) Although this command is optional, it is recommended that it be configured to specify an ACL that is to be applied to the device when the device switches to quiet mode. When the device is in quiet mode, all login requests are denied and the only available connection is through the console.
		If this command is not configured, then the default ACL **sl_def_acl** is created on the device. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.
		For example:
		`Device# show access-lists sl_def_acl`
		`Extended IP access list sl_def_acl`
		`10 deny tcp any any eq telnet`
		`20 deny tcp any any eq www`
		`30 deny tcp any any eq 22`
		`40 permit ip any any`

	Command or Action	Purpose
Step 5	**login delay** *seconds* **Example:** `Device(config)# login delay 10`	(Optional) Configures a delay between successive login attempts.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**show login failures** **Example:** `Device# show login`	Displays login parameters. • **failures** --Displays information related only to failed login attempts.

Verifying Login Parameters

Use this task to verify the applied login configuration and present login status on your device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show login failures** **Example:** `Device# show login`	Displays login parameters. • **failures** --Displays information related only to failed login attempts.

Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Device# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for**command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; five login requests have already failed.

```
Device# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the device is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Device# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100
 seconds.
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

The following sample output from **show login failures** command shows all failed login attempts on the device:

```
Device# show login failures

Information about login failure's with the device
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Feb 24 2019
try2          10.1.1.2        23    1     21:52:52 UTC Sun Feb 23 2019
```

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Device# show login failures

*** No logged failed login attempts with the device.***
```

Configuration Examples for Login Enhancements-Login Block

Example: Configuring Login Parameters

The following example shows how to configure your device to enter a 100 second quiet period if 15 failed login attempts is exceeded within 100 seconds; all login requests are denied during the quiet period except hosts from the ACL “myacl.”

```
Device> enable
Device# configure terminal
Device(config)# login block-for 100 attempts 15 within 100
Device(config)# login quiet-mode access-class myacl
Device(config)# end
```

Feature History for Login Enhancements-Login Block

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	Login Enhancements -Login Block	The Login Enhancements-Login Block feature allows users to enhance the security of a router by configuring options to automatically block further login attempts when a possible DoS attack is detected. Support for this feature was introduced on all the models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Cupertino 17.7.1	Login Enhancements -Login Block	Support for this feature was introduced on the C9500X-28C8D model of Cisco Catalyst 9500 Series Switches.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.