Cisco IOS Login Enhancements (Login Block)

First Published: August 2005
Last Updated: March 14, 2011

The Cisco IOS 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 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for Cisco IOS Login Enhancements (Login Block)” section on page 7.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

- Information About Cisco IOS Login Enhancements, page 2
- How to Configure Cisco IOS Login Enhancements, page 3
- Configuration Examples for Login Parameters, page 5
- Additional References, page 6
- Feature Information for Cisco IOS Login Enhancements (Login Block), page 7
Information About Cisco IOS Login Enhancements

- Protecting Against Denial of Service and Dictionary Login Attacks
- Login Enhancements Functionality Overview, page 2

Protecting Against Denial of Service and Dictionary Login Attacks

Connecting to a routing 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 routing 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.

Login Enhancements Functionality Overview

- Delays Between Successive Login Attempts
- Login Shutdown If DoS Attacks Are Suspected

Delays Between Successive Login Attempts

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

- Through the \texttt{auto secure} command. If you enable the AutoSecure feature, the default login delay time of one second is automatically enforced.
- Through the \texttt{login block-for} command. You must enter this command before issuing the \texttt{login delay} command. If you enter only the \texttt{login block-for} command, the default login delay time of one second is automatically enforced.
- Through the new global configuration mode command, \texttt{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 Cisco IOS 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 \texttt{login block-for}. The predefined ACL that is excluded from the quiet period can be specified through the new global configuration mode command \texttt{login quiet-mode access-class}.

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

**How to Configure Cisco IOS Login Enhancements**

- Configuring Login Parameters, page 3 (Required)
- Verifying Login Parameters, page 5 (Optional)

**Configuring Login Parameters**

Use this task to configure your Cisco IOS 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 \texttt{login block-for} command, which enables default login functionality, before using any other login commands. After the \texttt{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 \texttt{login quiet-mode access-class} command is issued.

**SUMMARY STEPS**

1. \texttt{enable}
2. \texttt{configure terminal}
3. \texttt{login block-for seconds attempts tries within seconds}
4. \texttt{login quiet-mode access-class \{acl-name \ acl-number\}}
5. \texttt{login delay seconds}
6. \texttt{exit}
7.
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> login block-for seconds attempts tries within seconds</td>
<td>Configures your Cisco IOS device for login parameters that help provide DoS detection.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# login block-for 100 attempts 2 within 100</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> This command must be issued before any other login command can be used.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> login quiet-mode access-class (acl-name</td>
<td>(Optional) Although this command is optional, it is recommended that it be configured to specify an ACL that is to be applied to the router when the router switches to quiet mode. When the router 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 router. 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:</td>
</tr>
<tr>
<td>acl-number)</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# login quiet-mode access-class myacl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> login delay seconds</td>
<td>(Optional) Configures a delay between successive login attempts.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# login delay 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show login</td>
<td>Displays login parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show login</td>
<td></td>
</tr>
<tr>
<td>• failures—Displays information related only to failed login attempts.</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Login Parameters

- Setting Login Parameters: Example, page 5
- Showing login Parameters: Example, page 5

Setting Login Parameters: Example

The following example shows how to configure your router 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.”

Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class myacl

Showing login Parameters: Example

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

Router# 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.

Router# 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 router 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.

Router# 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 router:

```plaintext
Router# 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 Mar 9 2003
try2       10.1.1.2        23   1    21:52:52 UTC Sun Mar 9 2003
```

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

```plaintext
Router# show login failures

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

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoSecure</td>
<td>“AutoSecure” feature module.</td>
</tr>
<tr>
<td>Secure Management/Administrative Access</td>
<td>“Role-Based CLI Access” feature module.</td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>download documentation, software, and tools. Use these resources to</td>
<td></td>
</tr>
<tr>
<td>install and configure the software and to troubleshoot and resolve</td>
<td></td>
</tr>
<tr>
<td>technical issues with Cisco products and technologies. Access to most</td>
<td></td>
</tr>
<tr>
<td>tools on the Cisco Support and Documentation website requires a Cisco.com</td>
<td></td>
</tr>
<tr>
<td>user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
Feature Information for Cisco IOS Login Enhancements (Login Block)

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Login Enhancements (Login Block)</td>
<td>12.3(4)T, 12.2(25)S, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXH, 12.4(15)T1</td>
<td>The Cisco IOS 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. This feature was introduced in Cisco IOS Release 12.3(4)T. This feature was integrated into Cisco IOS Release 12.2(25)S. This feature was integrated into Cisco IOS Release 12.2(33)SRA. Support for HTTP login blocking was integrated into Cisco IOS Release 12.2(33)SRB, 12.2(33)SXH, 12.4(15)T1.</td>
</tr>
</tbody>
</table>