Controlling Access to a Virtual Terminal Line

You can control who can access the virtual terminal lines (vtys) to a router by applying an access list to inbound vtys. You can also control the destinations that the vtys from a router can reach by applying an access list to outbound vtys.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Restrictions for Controlling Access to a Virtual Terminal Line

When you apply an access list to a vty (by using the **access-class** command), the access list must be a numbered access list, not a named access list.

Information About Controlling Access to a Virtual Terminal Line

Benefits of Controlling Access to a Virtual Terminal Line

By applying an access list to an inbound vty, you can control who can access the lines to a router. By applying an access list to an outbound vty, you can control the destinations that the lines from a router can reach.

How to Control Access to a Virtual Terminal Line

Controlling Inbound Access to a vty

Perform this task when you want to control access to a vty coming into the router by using an access list. Access lists are very flexible; this task illustrates one **access-list deny** command and one **access-list permit**command. You will decide how many of each command you should use and their order to achieve the restrictions you want.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]
4. **access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**}[**log**]
5. **line vty** *line-number* [*ending-line-number*]
6. **access-class** *access-list-number* **in** [**vrf-also**]
7. **exit**
8. Repeat Steps 5 and 6 for each line to set identical restrictions on all the vtys because a user can connect to any of them.
9. **end**
10. **show line** [*line-number* | **summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**] **Example:** `Router(config)# access-list 1 deny 172.16.7.34`	(Optional) Denies the specified source based on a source address and wildcard mask. • If the *source-wildcard* is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the keyword **any** as a substitute for the *source source-wildcard*to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, host 172.16.7.34 is denied passing the access list.
Step 4	**access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**}[**log**] **Example:** `Router(config)# access-list 1 permit 172.16.0.0 0.0.255.255`	Permits the specified source based on a source address and wildcard mask. • If the *source-wildcard* is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the keyword **any** as a substitute for the *source source-wildcard*to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, hosts on network 172.16.0.0 (other than the host denied in the prior step) pass the access list, meaning they can access the vtys identified in the **line** command.
Step 5	**line vty** *line-number* [*ending-line-number*] **Example:** `Router(config)# line vty 5 10`	Identifies a specific line for configuration and enters line configuration mode. • Entering the **line** command with the optional line type **vty** designates the line number as a relative line number. • You also can use the **line** command without specifying a line type. In this case, the line number is treated as an absolute line number.
Step 6	**access-class** *access-list-number* **in** [**vrf-also**] **Example:** `Router(config-line)# access-class 1 in vrf-also`	Restricts incoming connections between a particular vty (into a Cisco device) and the networking devices associated with addresses in the access list. • If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VPN routing and forwarding (VRF) instance are rejected.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-line)# exit`	Returns the user to the next highest configuration mode.
Step 8	Repeat Steps 5 and 6 for each line to set identical restrictions on all the vtys because a user can connect to any of them.	If you indicated the full range of vty lines in Step 5 with the **line** command, you do not need to repeat Steps 5 and 6.

Step 9	**end**
	Example:
	`Router(config-line)# end`
		Returns the user to privileged EXEC mode.

Step 10	**show line** [*line-number* | **summary**] **Example:** `Router# show line 5`	Displays parameters of a terminal line.

Controlling Outbound Access to a vty

Perform this task when you want to control access from a vty to a destination. Access lists are very flexible; this task illustrates one **access-list deny** command and one **access-list permit**command. You will decide how many of each command you should use and their order to achieve the restrictions you want.

When a standard access list is applied to a line with the **access-class out**command, the address specified in the access list is not a source address (as it is in an access list applied to an interface), but a destination address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny** {*destination* [*destination-wildcard*] | **any**} [**log**]
4. **access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **line vty** *line-number* [*ending-line-number*]
6. **access-class** *access-list-number* **out**
7. **exit**
8. Repeat Steps 5 and 6 for each line to set identical restrictions on all the vtys because a user can connect to any of them.
9. **end**
10. **show line** [*line-number* | **summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* **deny** {*destination* [*destination-wildcard*] | **any**} [**log**] **Example:** `Router(config)# access-list 2 deny 172.16.7.34`	Denies line access to the specified destination based on a destination address and wildcard mask. • If the *destination-wildcard* is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the keyword **any** as a substitute for the *destination destination-wildcard*to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, host 172.16.7.34 is denied passing the access list, meaning the line cannot connect to it.
Step 4	**access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**] **Example:** `Router(config)# access-list 2 permit 172.16.0.0 0.0.255.255`	Permits the specified source based on a source address and wildcard mask. • If the *source-wildcard* is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the keyword **any** as a substitute for the *source source-wildcard*to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, hosts on network 172.16.0.0 (other than the host denied in the prior step) pass the access list, meaning they can be connected to by the vtys identified in the **line** command.
Step 5	**line vty** *line-number* [*ending-line-number*] **Example:** `Router(config)# line vty 5 10`	Identifies a specific line for configuration and enter line configuration mode. • Entering the **line** command with the optional line type **vty** designates the line number as a relative line number. • You also can use the **line** command without specifying a line type. In this case, the line number is treated as an absolute line number.

	Command or Action	Purpose
Step 6	**access-class** *access-list-number* **out** **Example:** `Router(config-line)# access-class 2 out`	Restricts connections between a particular vty (into a Cisco device) out to the networking devices associated with addresses in the access list.
Step 7	**exit** **Example:** `Router(config-line)# exit`	Returns the user to the next highest configuration mode.
Step 8	Repeat Steps 5 and 6 for each line to set identical restrictions on all the vtys because a user can connect to any of them.	If you indicated the full range of vtys in Step 5 with the **line** command, you do not need to repeat Steps 5 and 6.

Step 9	**end**
	Example:
	`Router(config-line)# end`
		Returns the user to privileged EXEC mode.

Step 10	**show line** [*line-number* | **summary**] **Example:** `Router# show line 5`	Displays parameters of a terminal line.

Configuration Examples for Controlling Access to a Virtual Terminal Line

Example Controlling Inbound Access on vtys

The following example defines an access list that permits only hosts on network 172.19.5.0 to connect to the virtual terminal lines 1 through 5 on the router. Because the **vty** keyword is omitted from the **line** command, the line numbers 1 through 5 are absolute line numbers.

```
access-list 12 permit 172.19.5.0 0.0.0.255
line 1 5
 access-class 12 in
```

Example Controlling Outbound Access on vtys

The following example defines an access list that denies connections to networks other than network 171.20.0.0 on terminal lines 1 through 5. Because the **vty** keyword is omitted from the **line** command, the line numbers 1 through 5 are absolute line numbers.

```
access-list 10 permit 172.20.0.0 0.0.255.255
line 1 5
 access-class 10 out
```

Where to Go Next

You can further secure a vty by configuring a password with the **password** line configuration command. See the **password** (line configuration) command in the *Cisco IOS Security Command Reference*.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring a password on a line	*Cisco IOS Security Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Controlling Access to a Virtual Terminal Line

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 1: Feature Information for Controlling Access to a Virtual Terminal Line

Feature Name	Releases	Feature Configuration Information
Controlling Access to a Virtual Terminal Line	12.0(32)S4	You can control who can access the virtual terminal lines (vtys) to a router by applying an access list to inbound vtys. You can also control the destinations that the vtys from a router can reach by applying an access list to outbound vtys.