ip source-track

To enable IP source tracking for a specified host, use the **ip source-track** command in global configuration mode. To disable IP source tracking, use the **no** form of this command.

ip source-track *ip-address*

no ip source-track *ip-address*

Syntax Description

ip-address	Destination IP address of the host that is to be tracked.

Defaults

IP address tracking is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IP source tracking allows you to gather information about the traffic that is flowing to a host that is suspected of being under attack. It also allows you to easily trace a denial-of-service (DoS) attack to its entry point into the network.

After you have identified the destination that is being attacked, enable tracking for the destination address on the whole router by entering the **ip source-track** command.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
ip source-track export-interval	Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.
ip source-track syslog-interval	Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track address-limit

To configure the maximum number of destination hosts that can be simultaneously tracked at any given moment, use the **ip source-track address-limit** command in global configuration mode. To cancel this administrative limit and return to the default, use the **no** form of this command.

ip source-track address-limit *number*

no ip source-track address-limit *number*

Syntax Description

number	Maximum number of hosts that can be tracked.

Defaults

An unlimited number of hosts can be tracked.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you have configured at least one destination IP address for source tracking (via the **ip source-track** command), you can limit the number of destination IP addresses that can be tracked via the **ip source-track address-limit** command.

Examples

The following example shows how to configure IP source tracking for data that flows to host 100.10.1.1 and limit IP source tracking to 10 IP addresses:

```
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track address-limit 10
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip source-track export-interval

To set the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the route processor (RP), use the **ip source-track export-interval** command in global configuration mode. To return to default functionality, use the **no** form of this command.

ip source-track export-interval *number*

no ip source-track export-interval *number*

Syntax Description

number	Number of seconds that pass before IP source tracking statistics are exported.

Defaults

Traffic flow information is exported from the line card to the RP every 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip source-track export-interval** command to specify the frequency in which IP source tracking information is sent to the RP for viewing.

Note This command can be issued only on distributed platforms such as the gigabit route processor (GRP) and the route switch processor (RSP).

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
```

```
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track syslog-interval

To set the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device, use the **ip source-track syslog-interval** command in global configuration mode. To cancel this setting and disable syslog generation, use the **no** form of this command.

ip source-track syslog-interval *number*

no ip source-track syslog-interval *number*

Syntax Description

number	IP address of the destination that is to be tracked.

Defaults

Syslog messages are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip source-track syslog-interval** command to track the source interfaces of traffic that are destined to a particular address.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]

no ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]

Syntax Description

timeout	(Optional) The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0–4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
seconds	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
authentication-retries	(Optional) The number of attempts after which the interface is reset.
integer	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

Command Default

SSH control parameters are set to default router values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1) T.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa** command.

Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh break-string

To configure a string that, when received from a Secure Shell (SSH) client, will cause the Cisco IOS SSH server to transmit a break signal out an asynchronous line, use the **ip ssh break-string** command in global configuration mode. To remove the string, use the **no** form of this command.

ip ssh break-string *string*

no ip ssh break-string *string*

Syntax Description

string	Any sequence of characters not including embedded whitespace. Include control characters by prefixing them with ^V (control/V) or denote them using the \000 notation (that is, a backslash followed by the the ASCII value of the character in three octal digits.)

Defaults

Break signal is not enabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

Note This break string is used only for SSH sessions that are outbound on physical lines using the SSH Terminal-Line Access feature. This break string is not used by the Cisco IOS SSH client, nor is it used by the Cisco IOS SSH server when the server uses a virtual terminal (VTY) line. This break string does not provide any interoperability with the method that is described in the Internet Engineering Task Force (IETF) Internet-Draft “Session Channel Break Extension” (draft-ietf-secsh-break-02.txt).

Note In some versions of Cisco IOS, if the SSH break string is set to a single character, the Cisco IOS server will not immediately process that character as a break signal on receipt of that character but will delay until it has received a subsequent character. A break string of two or more characters will be immediately processed as a break signal after the last character in the string has been received from the SSH client.

Examples

The following example shows that the control-B character (ASCII 2) has been set as the SSH break string:

```
Router (config)# ip ssh break-string \002
```

Related Commands

Command	Description
ip ssh port	Enables SSH access to TTY lines.

ip ssh dh min size

To configure the modulus size on the Secure Shell (SSH) server, use the **ip ssh dh min size** command in privileged EXEC mode. To disable the configuration, use the **no** form of this command.

ip ssh dh min size [*number*]

no ip ssh dh min size

Syntax Description

number	(Optional) Minimum number of bits in the key size. The default is 1024.

Command Default

Bit key support is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

Use the **ip ssh dh min size** command to ensure that the CLI is successfully parsed from either the client side or the server side.

Examples

The following example shows how to set the minimum modulus size to 2048 bits:

```
Router> enable
Router# ip ssh dh min size 2048
```

Related Commands

Command	Description
show ip ssh	Displays the status of SSH server connections.

ip ssh dscp

To specify the IP differentiated services code point (DSCP) value that can be set for a Secure Shell (SSH) configuration, use the **ip ssh dscp** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh dscp *number*

no ip ssh dscp *number*

Syntax Description

number	Value that can be set. The default value is 0 (zero). • *number*—0 through 63.

Command Default

The IP DSCP value is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)S	This command was introduced.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

IP DSCP values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

Examples

The following example shows that the DSCP value is set to 35:

```
Router(config)# ip ssh dscp 35
```

Related Commands

Command	Description
ip ssh precedence	Specifies the IP precedence value that may be set.

ip ssh maxstartups

To set the maximum concurrent sessions allowed on a Secure Shell (SSH), use the **ip ssh maxstartups** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip ssh maxstartups [*number*]

no ip ssh maxstartups [*number*]

Syntax Description

number	(Optional) Number of connections to be accepted concurrently. The range is from 2 to 128. The default is 128.

Command Default

The number of maximum concurrent sessions is 128.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

You must create RSA keys to enable SSH. The RSA key must be at least 768 bits for SSHv2.

Examples

The following example shows how to set the maximum concurrent sessions allowed on a SSH to 100:

```
Router# configure terminal
Router(config)# ip ssh maxstartups 100
```

Related Commands

Command	Description
debug ip ssh	Displays debugging messages for SSH.
ip ssh	Configures SSH control parameters on your router.

ip ssh port

To enable secure access to tty (asynchronous) lines, use the **ip ssh port** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip ssh port *por-tnum* **rotary** *group*

no ip ssh port *por-tnum* **rotary** *group*

Syntax Description

port-num	Specifies the port, such as 2001, to which Secure Shell (SSH) needs to connect.
rotary *group*	Specifies the defined rotary that should search for a valid name.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The **ip ssh port** command supports a functionality that replaces reverse Telnet with SSH. Use this command to securely access the devices attached to the serial ports of a router and to perform the following tasks:

- Connect to a router with multiple terminal lines that are connected to consoles of other devices.
- Allow network available modems to be securely accessed for dial-out.

Examples

The following example shows how to configure the SSH Terminal-Line Access feature on a modem that is used for dial-out on lines 1 through 200:

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh

ip ssh port 2000 rotary 1
```

The following example shows how to configure the SSH Terminal-Line Access feature to access the console ports of various devices that are attached to the serial ports of the router. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used, and the port (line) mappings of the configuration are as follows: Port 2001 = Line 1, Port 2002 = Line 2, and Port 2003 = Line 3.

```
line 1
 no exec
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh

ip ssh port 2001 rotary 1 3
```

From any UNIX or UNIX-like device, the following command is typically used to form an SSH session:

```
ssh -c 3des -p 2002 router.example.com
```

This command will initiate an SSH session using the Triple DES cipher to the device known as "router.example.com," which uses port 2002. This device will connect to the device on Line 2, which was associated with port 2002. Similarly, many Windows SSH packages have related methods of selecting the cipher and the port for this access.

Related Commands

Command	Description
crypto key generate rsa	Enables the SSH server.
debug ip ssh	Displays debugging messages for SSH.
ip ssh	Configures SSH control variables on your router.
line	Identifies a specific line for configuration and begins the command in line configuration mode.
rotary	Defines a group of lines consisting of one or more lines.
ssh	Starts an encrypted session with a remote networking device.
transport input	Defines which protocols to use to connect to a specific line of the router.

ip ssh precedence

To specify the IP precedence value that can be set for a Secure Shell (SSH) configuration, use the **ip ssh precedence** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh precedence *number*

no ip ssh precedence *number*

Syntax Description

number	Value that can be set. The default value is 0 (zero). • *number*—0 through 7.

Command Default

The IP precedence value is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(20)S	This command was introduced.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

IP precedence values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

Examples

The following example shows that up to six IP precedence values can be set:

```
Router(config)# ip precedence value 6
```

Related Commands

Command	Description
ip ssh dscp	Specifies the IP DSCP value that can be set for an SSH configuration.

ip ssh pubkey-chain

To configure Secure Shell RSA (SSH-RSA) keys for user and server authentication on the SSH server, use the **ip ssh pubkey-chain** command in global configuration mode. To remove SSH-RSA keys for user and server authentication on the SSH server, use the **no** form of this command.

ip ssh pubkey-chain

no ip ssh pubkey-chain

Syntax Description

This command has no arguments or keywords.

Command Default

SSH-RSA keys are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **ip ssh pubkey-chain** command to ensure SSH server and user public key authentication.

Examples

The following example shows how to enable public key generation:

```
Router(config)# ip ssh pubkey-chain
```

Related Commands

Command	Description
ip ssh stricthostkeycheck	Enables strict host key checking on the SSH server.

ip ssh rsa keypair-name

To specify which Rivest, Shimar, and Adelman (RSA) key pair to use for a Secure Shell (SSH) connection, use the **ip ssh rsa keypair-name** command in global configuration mode. To disable the key pair that was configured, use the **no** form of this command.

ip ssh rsa keypair-name *keypair-name*

no ip ssh rsa keypair-name *keypair-name*

Syntax Description

keypair-name	Name of the key pair.

Command Default

If this command is not configured, SSH will use the first RSA key pair that is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Using the **ip ssh rsa keypair-name** command, you can enable an SSH connection using RSA keys that you have configured using the *keypair-name* argument. Previously, SSH was tied to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). The previous behavior still exists, but by using the **ip ssh rsa keypair-name** command, you can overcome that behavior. If you configure the **ip ssh rsa keypair-name** command with a key pair name, SSH is enabled if the key pair exists, or SSH will be enabled if the key pair is generated later. If you use this command, you are not forced to configure a hostname and a domain name.

Note A Cisco IOS router can have many RSA key pairs.

Examples

The following example shows how to specify the RSA key pair "sshkeys" for an SSH connection:

```
Router# configure terminal
Router(config)# ip ssh rsa keypair-name sshkeys
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh version	Specifies the version of SSH to be run on a router.
show ip ssh	Displays the SSH connections of your router.

ip ssh source-interface

To specify the IP address of an interface as the source address for a Secure Shell (SSH) client device, use the **ip ssh source-interface** command in global configuration mode. To remove the IP address as the source address, use the **no** form of this command.

ip ssh source-interface *interface*

no ip ssh source-interface *interface*

Syntax Description

interface	The interface whose address is used as the source address for the SSH client.

Defaults

The address of the closest interface to the destination is used as the source address (the closest interface is the output interface through which the SSH packet is sent).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

By specifying this command, you can force the SSH client to use the IP address of the source interface as the source address.

Examples

In the following example, the IP address assigned to Ethernet interface 0 will be used as the source address for the SSH client:

```
ip ssh source-interface ethernet0
```

ip ssh stricthostkeycheck

To enable strict host key checking on the Secure Shell (SSH) server, use the **ip ssh stricthostcheck** command in global configuration mode. To disable strict host key checking, use the **no** form of this command.

ip ssh stricthostkeycheck

no ip ssh stricthostkeycheck

Syntax Description

This command has no arguments or keywords.

Command Default

Strict host key checking on the SSH server is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **ip ssh stricthostkeycheck** command to ensure SSH server side strict checking. Configuring the **ip ssh stricthostkeycheck** command authenticates all servers.

Note

- This command is not available on SSH Version 1.
- If the **ip ssh pubkey-chain** command is not configured, the **ip ssh stricthostkeycheck** command will lead to connection failure in SSH Version 2.

Examples

The following example shows how to enable strict host key checking:

```
Router(config)# ip ssh stricthostkeycheck
```

Related Commands

Command	Description
ip ssh pubkey-chain	Configures SSH-RSA keys for user and server authentication on the SSH server.

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version** command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

Syntax Description

1	(Optional) Router runs only SSH Version 1.
2	(Optional) Router runs only SSH Version 2.

Defaults

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh rsa keypair-name	Specifies which RSA key pair to use for a SSH connection.
show ip ssh	Displays the SSH connections of your router.

ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration or server-group configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Syntax Description

subinterface-name	Name of the interface that TACACS+ uses for all of its outgoing packets.

Command Default

None

Command Modes

Global configuration (config)

Server-group configuration (server-group)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was introduced in server-group configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use this command to set the IP address of a subinterface for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a *down* state, TACACS+ reverts to the default. To avoid this situation, add an IP address to the subinterface or bring the interface to the *up* state.

Note This command can be configured globally or in server-group configuration mode. If this command is configured in the server-group configuration mode, the IP address of the specified interface is used for packets that are going only to servers that are defined in that server group. If this command is not configured in server-group configuration mode, the global configuration applies.

Examples

The following example makes TACACS+ use the IP address of subinterface "s2" for all outgoing TACACS+ packets:

```
ip tacacs source-interface s2
```

In the following example, TACACS+ is to use the IP address of Loopback0 for packets that are going only to server 10.1.1.1:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
server-private	Configures the IP address of the private RADIUS or TACACS+ server for the group server.

ip tcp intercept connection-timeout

To change how long a TCP connection will be managed by the TCP intercept after no activity, use the **ip tcp intercept connection-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept connection-timeout *seconds*

no ip tcp intercept connection-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24 hours).

Defaults

86,400 seconds (24 hours)

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip tcp intercept connection-timeout** command to change how long a TCP connection will be managed by the TCP intercept after a period of inactivity.

Examples

The following example sets the software to manage the connection for 12 hours (43,200 seconds) after no activity:

```
ip tcp intercept connection-timeout 43200
```

ip tcp intercept drop-mode

To set the TCP intercept drop mode, use the **ip tcp intercept drop-mode** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept drop-mode [**oldest | random**]

no ip tcp intercept drop-mode [**oldest | random**]

Syntax Description

oldest	(Optional) Software drops the oldest partial connection. This is the default.
random	(Optional) Software drops a randomly selected partial connection.

Defaults

oldest

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature becomes more aggressive. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection will be cut in half).

Note that the 1100 thresholds can be configured with the **ip tcp intercept max-incomplete high** and **ip tcp intercept one-minute high** commands.

Use the **ip tcp intercept drop-mode** command to change the dropping strategy from oldest to a random drop.

Examples

The following example sets the drop mode to random:

```
ip tcp intercept drop-mode random
```

Related Commands

Command	Description
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minute sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept finrst-timeout

To change how long after receipt of a reset or FIN-exchange the software ceases to manage the connection, use the **ip tcp intercept finrst-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept finrst-timeout *seconds*

no ip tcp intercept finrst-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Even after the two ends of the connection are joined, the software intercepts packets being sent back and forth. Use this command if you need to adjust how soon after receiving a reset or FIN-exchange the software stops intercepting packets.

Examples

The following example sets the software to wait for 10 seconds before it leaves intercept mode:

```
ip tcp intercept finrst-timeout 10
```

ip tcp intercept list

To enable TCP intercept, use the **ip tcp intercept list** command in global configuration mode. To disable TCP intercept, use the **no** form of this command.

ip tcp intercept list *access-list-number*

no ip tcp intercept list *access-list-number*

Syntax Description

access-list-number	Extended access list number in the range from 100 to 199.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The TCP intercept feature intercepts TCP connection attempts and shields servers from TCP SYN-flood attacks, also known as denial-of-service attacks.

TCP packets matching the access list are presented to the TCP intercept code for processing, as determined by the **ip tcp intercept mode** command. The TCP intercept code either intercepts or watches the connections.

To have all TCP connection attempts submitted to the TCP intercept code, have the access list match everything.

Examples

The following example configuration defines access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
ip tcp intercept mode	Changes the TCP intercept mode.

Command	Description
show tcp intercept connections	Displays TCP incomplete and established connections.
show tcp intercept statistics	Displays TCP intercept statistics.

ip tcp intercept max-incomplete

To define either the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete **low** *number* **high** *number*

no ip tcp intercept max-incomplete [**low** *number* **high** *number*]

Syntax Description

low *number*	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900
high *number*	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

Command Default

The number of incomplete connections below which the software leaves aggressive mode is 900.

The maximum number of incomplete connections allowed before the software enters aggressive mode is 1100.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the **ip tcp intercept max-incomplete low** and the **ip tcp intercept max-incomplete high** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if *both* the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if *either* the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the **ip tcp intercept one-minute** command and the number of incomplete connections may be defined by the **ip tcp intercept max-incomplete** command.

Characteristics of Aggressive Mode

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.

- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
- The watch-timeout period is reduced from 30 seconds to 15 seconds.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000 and allows 1500 incomplete connections before the software enters aggressive mode. The running configuration is also shown.

```
Router(config)# ip tcp intercept max-incomplete low 1000 high 1500
Router(config)# show running config | i ip tcp

     ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept one-minute	Defines the number of connection requests below which the software leaves aggressive mode and the number of connection requests received before the software enters aggressive mode.

ip tcp intercept max-incomplete high

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept max-incomplete high** command is replaced by the **ip tcp intercept max-incomplete** command. See the **ip tcp intercept max-incomplete** command for more information.

To define the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete high** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete high *number*

no ip tcp intercept max-incomplete high [*number*]

Syntax Description

number	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

Defaults

1100 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept max-incomplete** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept max-incomplete** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept max-incomplete high** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept max-incomplete high** command has been replaced by the **ip tcp intercept max-incomplete** command.

If the number of incomplete connections exceeds the *number* configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.

- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of ip tcp intercept one-minute low and **ip tcp intercept max-incomplete low**, aggressive mode ends.

The software will back off from its aggressive mode when the number of incomplete connections falls below the number specified by the **ip tcp intercept max-incomplete low** command.

Examples

The following example allows 1500 incomplete connections before the software enters aggressive mode:

```
ip tcp intercept max-incomplete high 1500
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept max-incomplete low

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept max-incomplete low** command is replaced by the **ip tcp intercept max-incomplete** command. See the **ip tcp intercept max-incomplete** command for more information.

To define the number of incomplete connections below which the software leaves aggressive mode, use the **ip tcp intercept max-incomplete low** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete low *number*

no ip tcp intercept max-incomplete low [*number*]

Syntax Description

number	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900.

Defaults

900 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept max-incomplete** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept max-incomplete** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH, or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept max-incomplete low** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept max-incomplete high** command has been replaced by the **ip tcp intercept max-incomplete** command.

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept max-incomplete high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000:

```
ip tcp intercept max-incomplete low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept mode

To change the TCP intercept mode, use the **ip tcp intercept mode** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept mode {**intercept** | **watch**}

no ip tcp intercept mode [**intercept** | **watch**]

Syntax Description

intercept	Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.
watch	Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.

Defaults

intercept

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When TCP intercept is enabled, it operates in intercept mode by default. In intercept mode, the software actively intercepts TCP SYN packets from clients to servers that match the specified access list. For each SYN, the software responds on behalf of the server with an ACK and SYN, and waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is sent to the server, and the code then performs a three-way handshake with the server. Then the two half-connections are joined.

In watch mode, the software allows connection attempts to pass through the router, but watches them until they become established. If they fail to become established in 30 seconds (or the value set by the **ip tcp intercept watch-timeout** command), a Reset is sent to the server to clear its state.

Examples

The following example sets the mode to watch mode:

```
ip tcp intercept mode watch
```

Related Commands

Command	Description
ip tcp intercept watch-timeout	Defines how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server.

ip tcp intercept one-minute

To define both the number of connection requests below which the software leaves aggressive mode and the number of connection requests that can be received before the software enters aggressive mode, use the **ip tcp intercept one-minute** command in global configuration mode. To restore the default connection request settings, use the **no** form of this command.

ip tcp intercept one-minute low *number* **high** *number*

no ip tcp intercept one-minute [**low** *number* **high** *number*]

Syntax Description

low *number*	Specifies the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.
high *number*	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

Command Default

The default number of connection requests below which the software leaves aggressive mode is 900.

The default number of connection requests received before the software enters aggressive mode is 1100.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the **ip tcp intercept one-minute low** and the **ip tcp intercept one-minute high** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if *both* the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if *either* the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the **ip tcp intercept one-minute** command and the number of incomplete connections may be defined by the **ip tcp intercept max-incomplete** command. The default number of connection requests

Characteristics of Aggressive Mode

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.

- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
- The watch-timeout period is reduced from 30 seconds to 15 seconds.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000 and allows 1400 connection requests before the software enters aggressive mode. The the running configuration is then shown.

```
Router(config)# ip tcp intercept one-minute low 1000 high 1400
Router(config)# show running configuration | i ip tcp

     ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete	Defines the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode.

ip tcp intercept one-minute high

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T the **ip tcp intercept one-minute high** command is replaced by the **ip tcp intercept one-minute** command. See the **ip tcp intercept one-minute** command for more information.

To define the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode, use the **ip tcp intercept one-minute high** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute high *number*

no ip tcp intercept one-minute high [*number*]

Syntax Description

number	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

Defaults

1100 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept one-minute** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept one-minute** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept one-minute high** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept one-minute high** command has been replaced by the **ip tcp intercept one-minute** command.

If the number of connection requests exceeds the *number* value configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

Examples

The following example allows 1400 connection requests before the software enters aggressive mode:

```
ip tcp intercept one-minute high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept one-minute low

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept one-minute low** command is replaced by the **ip tcp intercept one-minute** command. See the **ip tcp intercept one-minute** command for more information.

To define the number of connection requests below which the software leaves aggressive mode, use the **ip tcp intercept one-minute low** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute low *number*

no ip tcp intercept one-minute low [*number*]

Syntax Description

number	Defines the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.

Defaults

900 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept one-minute** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept one-minute** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept one-minute low** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept one-minute low** command has been replaced by the **ip tcp intercept one-minute** command.

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept one-minute high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000:

```
ip tcp intercept one-minute low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.

ip tcp intercept watch-timeout

To define how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server, use the **ip tcp intercept watch-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept watch-timeout *seconds*

no ip tcp intercept watch-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if you have set the TCP intercept to passive watch mode and you want to change the default time the connection is watched. During aggressive mode, the watch timeout time is cut in half.

Examples

The following example sets the software to wait 60 seconds for a watched connection to reach established state before sending a Reset to the server:

```
ip tcp intercept watch-timeout 60
```

Related Commands

Command	Description
ip tcp intercept mode	Changes the TCP intercept mode.

ip traffic-export apply

To apply an IP traffic export profile or an IP traffic capture profile to a specific interface, use the **ip traffic-export apply** command in interface configuration mode. To remove an IP traffic export profile or an IP traffic capture profile from an interface, use the **no** form of this command.

ip traffic-export apply *profile-name*

no ip traffic-export apply *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series

ip traffic-export apply *profile-name* **size** *size*

no ip traffic-export apply *profile-name*

Syntax Description

profile-name	Name of the profile that is to be applied to a specified interface. The *profile-name* argument must match a name that was specified in the **ip traffic-export profile** command.
size	Optional. Used in IP traffic capture mode to set up a local capture buffer.
size	Optional. Specifies the size of the local capture buffer, in bytes.

Defaults

If you do not use this command, a sucessfully configured profile is not active.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(11)T	This command was updated to incorporate the **size** keyword and *size* argument for IP traffic capture mode on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

After you configure at least one export profile, use the **ip traffic-export apply** command to activate IP traffic export on the specified ingress interface.

After you configure a capture profile, use the **ip traffic-export apply** command to activate IP traffic capture on the specified ingress interface, and to specify the size of the local capture buffer.

Examples

The following example shows how to apply the export profile “corp1” to interface Fast Ethernet 0/0.

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list spam_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to apply the capture profile “corp2” to interface Fast Ethernet 0/0, and specify a capture buffer of 10,000,000 bytes.

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

After a profile is activated on the interface, a logging message such as the following will appear:

```
%RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.
```

After a profile is removed from the interface, a logging message such as the following will appear:

```
%RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.
```

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

```
Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
traffic-export	Controls the operation of IP traffic capture mode.

ip traffic-export profile

To create or edit an IP traffic export profile or an IP traffic capture profile and enable the profile on an ingress interface, use the **ip traffic-export profile** command in global configuration mode. To remove an IP traffic export profile from your router configuration, use the **no** form of this command.

ip traffic-export profile *profile-name*

no ip traffic-export profile *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series Routers

ip traffic-export profile *profile-name* **mode** {**capture** | **export**}

no ip traffic-export profile *profile-name*

Syntax Description

profile-name	IP traffic export profile name.
mode {**capture** | **export**}	Specifies either capture or export mode. • **capture**—Captures data to memory. • **export**—Exports data to an interface.

Defaults

A profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(11)T	This command was updated to incorporate the **mode**, **capture**, and **export** keywords on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

The **ip traffic-export profile** command allows you to begin a profile that can be configured to capture or export IP packets as they arrive on or leave from a selected router ingress interface.

When exporting IP packets, a designated egress interface exports IP packets out of the router. So, the router can export unaltered IP packets to a directly connected device.

When capturing IP packets, the packets are stored in local router memory. They may then be dumped to an external device.

IP Traffic Export Profiles

All exported IP traffic configurations are specified by profiles, which consist of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic. You can configure a router with multiple profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two profiles to configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile** command.
- Submode configuration profile, which you configure using any of the following RITE commands—**bidirectional**, **incoming**, **interface**, **mac-address**, and **outgoing**.

Use **interface** and **mac-address** commands to successfully create a profile. If you do not issue these commands, the user will receive a profile incomplete messages such as the following:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile** command, which will activate it.

IP Traffic Capture Profiles

On the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers, you can also configure IP traffic capture. A captured IP traffic configuration is specified by a profile, which consists of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic.

The two profiles that you should configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile mode capture** command.
- Submode configuration profile, which you configure using any of the following RITE commands—**bidirectional**, **incoming**, **length**, and **outgoing**.

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile** command, which will activate it.

When the IP traffic capture profile is applied to an interface, use the **traffic-export** command to control the capture of the traffic.

Note Cisco IOS Release 12.4(9)T and 12.4(15)T cannot capture outgoing router-generated Internet Control Message Protocol (ICMP) or IPsec traffic.

Examples

The following example shows how to configure the profile “corp1,” which sends captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export 1 in every 50 packets and to allow incoming traffic only from the access control list (ACL) “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to configure the profile "corp2," which captures IP traffic and stores it in a local router memory buffer of 10,000,000 bytes. This profile also captures 1 in every 50 packets and allows incoming traffic only from the access control list (ACL) "ham_ACL."

```
Router(config)# ip traffic-export profile corp2 mode capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming export or capture traffic.
interface (RITE)	Specifies the outgoing interface for exporting traffic
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
length	Specifies the length of the packet in capture mode.
mac-address	Specifies the Ethernet address of the destination host in traffic export.
outgoing	Configures filtering for outgoing export or capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

ip trigger-authentication (global)

To enable the automated part of double authentication at a device, use the **ip trigger-authentication** command in global configuration mode. To disable the automated part of double authentication, use the **no** form of this command.

ip trigger-authentication [**timeout** *seconds*] [**port** *number*]

no ip trigger-authentication

Syntax Description

timeout *seconds*	(Optional) Specifies how frequently the local device sends a User Datagram Protocol (UDP) packet to the remote host to request the user's username and password (or PIN). The default is 90 seconds. See "The Timeout Keyword" in the Usage Guidelines section for details.
port *number*	(Optional) Specifies the UDP port to which the local router should send the UPD packet requesting the user's username and password (or PIN). The default is port 7500. See "The Port Keyword" in the Usage Guidelines section for details.

Defaults

The default timeout is 90 seconds, and the default port number is 7500.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure this command on the local device (router or network access server) that remote users dial in to. Use this command only if the local device has already been configured to provide double authentication; this command enables automation of the second authentication of double authentication.

The timeout Keyword

During the second authentication stage of double authentication—when the remote user is authenticated—the remote user must send a username and password (or PIN) to the local device. With automated double authentication, the local device sends a UDP packet to the remote user's host during the second user-authentication stage. This UDP packet triggers the remote host to launch a dialog box requesting a username and password (or PIN).

If the local device does not receive a valid response to the UDP packet within a timeout period, the local device will send another UDP packet. The device will continue to send UDP packets at the timeout intervals until it receives a response and can authenticate the user.

By default, the UDP packet timeout interval is 90 seconds. Use the **timeout** keyword to specify a different interval.

(This timeout also applies to how long entries will remain in the remote host table; see the **show ip trigger-authentication** command for details.)

The port Keyword

As described in the previous section, the local device sends a UDP packet to the remote user's host to request the user's username and password (or PIN). This UDP packet is sent to UDP port 7500 by default. (The remote host client software listens to UDP port 7500 by default.) If you need to change the port number because port 7500 is used by another application, you should change the port number using the **port** keyword. If you change the port number you need to change it in both places—both on the local device and in the remote host client software.

Examples

The following example globally enables automated double authentication and sets the timeout to 120 seconds:

```
ip trigger-authentication timeout 120
```

Related Commands

Command	Description
ip trigger-authentication (interface)	Specifies automated double authentication at an interface.
show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

ip trigger-authentication (interface)

To specify automated double authentication at an interface, use the **ip trigger-authentication** command in interface configuration mode. To turn off automated double authentication at an interface, use the **no** form of this command.

ip trigger-authentication

no ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

Automated double authentication is not enabled for specific interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure this command on the local router or network access server that remote users dial into. Use this command only if the local device has already been configured to provide double authentication and if automated double authentication has been enabled with the **ip trigger-authentication** (global) command.

This command causes double authentication to occur automatically when users dial into the interface.

Examples

The following example turns on automated double authentication at the ISDN BRI interface BRI0:

```
interface BRI0
 ip trigger-authentication
 encapsulation ppp
 ppp authentication chap
```

Related Commands

Command	Description
ip trigger-authentication (global)	Enables the automated part of double authentication at a device.

ip urlfilter alert

To enable URL filtering system alert messages, use the **ip urlfilter alert** command in global configuration mode. To disable the system alert, use the **no** form of this command.

ip urlfilter alert [**vrf** *vrf-name*]

no ip urlfilter alert

Syntax Description

vrf *vrf-name*	(Optional) Enables URL filtering system alert messages only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

URL filtering messages are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter alert** command to display system messages, such as a server entering allow mode, a server going down, or a URL that is too long for the lookup request.

Examples

The following example shows how to enable URL filtering alert messages:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Afterward, system alert messages such as the following are displayed:

```
%URLF-3-SERVER_DOWN:Connection to the URL filter server 10.92.0.9 is down
```

This level three LOG_ERR-type message is displayed when a configured URL filter server (UFS) goes down. When this happens, the firewall will mark the configured server as secondary and try to bring up one of the other secondary servers and mark that server as the primary server. If there is no other server configured, the firewall will enter into allow mode and display the URLF-3-ALLOW_MODE message described.

```
%URLF-3-ALLOW_MODE:Connection to all URL filter servers are down and ALLOW MODE is OFF
```

This LOG_ERR type message is displayed when all UFSs are down and the system enters into allow mode.

Note Whenever the system goes into allow mode (all filter servers are down), a periodic keepalive timer will be triggered that will try to bring up a server by opening a TCP connection.

```
%URLF-5-SERVER_UP:Connection to an URL filter server 10.92.0.9 is made, the system is
returning from ALLOW MODE
```

This LOG_NOTICE-type message is displayed when the UFSs are detected as being up and the system is returning from allow mode.

```
%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?
```

This LOG_WARNING-type message is displayed when the URL in a lookup request is too long; any URL longer than 3K will be dropped.

```
%URLF-4-MAX_REQ:The number of pending request exceeds the maximum limit <1000>
```

This LOG_WARNING-type message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.

ip urlfilter allowmode

To turn on the default mode (allow mode) of the filtering algorithm, use the **ip urlfilter allowmode** command in global configuration mode. To disable the default mode, use the **no** form of this command.

ip urlfilter allowmode [**on** | **off**] [**vrf** *vrf-name*]

no ip urlfilter allowmode [**on** | **off**]

Syntax Description

on	(Optional) Allow mode is on.
off	(Optional) Allow mode is off.
vrf *vrf-name*	(Optional) Turns on the default mode of the filtering algorithm only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Allow mode is off.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

The system will go into allow mode when connections to all vendor servers (Websense or N2H2) are down. The system will return to normal mode when a connection to at least one web vendor server is up. Allow mode directs your system to forward or drop all packets on the basis of the configurable allow mode setting: if allow mode is on and the vendor servers are down, the HTTP requests will be allowed to pass; if allow mode is off and the vendor servers are down, the HTTP requests will be forbidden.

Examples

The following example shows how to enable allow mode on your system:

```
ip urlfilter allowmode on
```

Afterward, the following alert message will be displayed when the system goes into allow mode:

```
%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE if OFF
```

The following alert message will be displayed when the system returns from allow mode:

```
%URLF-5-SERVER_UP: Connection to an URL filter server 12.0.0.3 is made, the system is
returning from allow mode
```

ip urlfilter audit-trail

To log messages into the syslog server or router, use the **ip urlfilter audit-trail** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip urlfilter audit-trail [**vrf** *vrf-name*]

no ip urlfilter audit-trail

Syntax Description

vrf *vrf-name*	(Optional) Logs messages into the syslog server or router only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter audit-trail** command to log messages such as URL request status (allow or deny) into your syslog server.

Examples

The following example shows how to enable syslog message logging:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 209.165.202.130
```

Afterward, audit trail messages such as the following are displayed and logged into the log server:

```
%URLF-6-SITE_ALLOWED:Client 209.165.201.15:12543 accessed server 10.76.82.21:8080
```

This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged in this case because the IP address of the request is found in the cache; thus, parsing the request and extracting the URL is a waste of time.

```
%URLF-4-SITE-BLOCKED: Access denied for the site 'www.sports.com'; client
209.165.200.230:34557 server 209.165.201.2:80
```

This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.

```
%URLF-6-URL_ALLOWED:Access allowed for URL http://www.N2H2.com/; client
209.165.200.230:54123  server 192.168.0.1:80
```

This message is logged for each URL request that is allowed by the vendor server (Websense or N2H2). It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

```
%URLF-6-URL_BLOCKED:Access denied URL http://www.google.com; client 209.165.200.230:54678
server 209.165.201.2:80
```

This message is logged for each URL request that is blocked by the vendor server. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

ip urlfilter cache

To configure cache parameters, use the **ip urlfilter cache** command in global configuration mode. To clear the configuration, use the **no** form of this command.

ip urlfilter cache number [**vrf** *vrf-name*]

no ip urlfilter cache number

Syntax Description

number	Maximum number of destination IP addresses that can be cached into the cache table. The default value is 5000.
vrf *vrf-name*	(Optional) Configures cache parameters only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Maximum number of destination IP addresses is 5000.

The cache table is cleared out every 12 hours.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

The cache table consists of the most recently requested IP addresses and respective authorization status for each IP address.

The caching algorithm involves three parameters—the maximum number of IP addresses that can be cached, an idle time, and an absolute time. The algorithm also involves two timers—idle timer and absolute timer. The idle timer is a small periodic timer (1 minute) that checks to see whether the number of cached IP addresses in the cache table exceeds 80 percent of the maximum limit. If the cached IP addresses have exceeded 80 percent, it will start removing idle entries; if it has not exceeded 80 percent, it will quit and wait for the next cycle. The absolute timer is a large periodic timer (1 hour) that is used to remove all of the elapsed entries. (The age of an elapsed entry is greater than the absolute time.) An elapsed entry will also be removed during cache lookup.

The idle time value is fixed at 10 minutes. The absolute time value is taken from the vendor server look-up response, which is often greater than 15 hours. The absolute value for cache entries made out of exclusive-domains is 12 hours. The maximum number of cache entries is configurable by enabling the **ip urlfilter cache** command.

Note The vendor server is not able to inform the Cisco IOS firewall of filtering policy changes in the database.

Examples

The following example shows how to configure the cache table to hold a maximum of five destination IP addresses:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

ip urlfilter exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the firewall does not have to send lookup requests to the vendor server, use the **ip urlfilter exclusive-domain** command in global configuration mode. To remove a domain name from the exclusive domain name list, use the **no** form of this command.

ip urlfilter exclusive-domain {**permit** | **deny**} *domain-name* [**vrf** *vrf-name*]

no ip urlfilter exclusive-domain {**permit** | **deny**} *domain-name*

Syntax Description

permit	Permits all traffic destined for the specified domain name.
deny	Blocks all traffic destined for the specified domain name.
domain-name	Domain name that is added or removed from the exclusive domain name list; for example, www.cisco.com.
vrf *vrf-name*	(Optional) Adds or removes a domain name only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

The **ip urlfilter exclusive-domain** command allows you to specify a list of domain names (exclusive domains) so that the firewall will not create a lookup request for the HTTP traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending look-up requests to the web server for HTTP traffic that is destined for a host that is completely allowed to all users.

Flexibility when entering domain names is also provided; that is, the user can enter the complete domain name or a partial domain name.

Complete Domain Name

If the user adds a complete domain name, such as “www.cisco.com,” to the exclusive domain list, all HTTP traffic whose URLs are destined for this domain (such as www.cisco.com/news and www.cisco.com/index) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Partial Domain Name

If the user adds only a partial domain name to the exclusive domain list, such as ".cisco.com," all URLs whose domain names end with this partial domain name (such as www.cisco.com/products and www.cisco.com/eng) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Examples

The following example shows how to add the complete domain name "www.cisco.com" to the exclusive domain name list. This configuration will block all traffic destined to the www.cisco.com domain.

```
ip urlfilter exclusive-domain deny www.cisco.com
```

The following example shows how to add the partial domain name ".cisco.com" to the exclusive domain name list. This configuration will permit all traffic destined to domains that end with .cisco.com.

```
ip urlfilter exclusive-domain permit .cisco.com
```

ip urlfilter max-request

To set the maximum number of outstanding requests that can exist at any given time, use the **ip urlfilter max-request** command in global configuration mode. To disable this function, use the **no** form of this command.

ip urlfilter max-request *number* [**vrf** *vrf-name*]

no ip urlfilter max-request *number*

Syntax Description

number	Maximum number of outstanding requests. The default value is 1000.
vrf *vrf-name*	(Optional) Sets the maximum number of outstanding requests only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Maximum number of requests is 1000.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

If the specified maximum number of outstanding requests is exceeded, new requests will be dropped.

Note Allow mode is not considered because it should be used only when servers are down.

Examples

The following example shows how to configure the maximum number of outstanding requests to 950:

```
ip inspect name url_filter http
ip urlfilter max-request 950
```

Related Commands

Command	Description
ip inspect name	Defines a set of inspection rules.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

ip urlfilter max-resp-pak

To configure the maximum number of HTTP responses that the firewall can keep in its packet buffer, use the **ip urlfilter max-resp-pak** command in global configuration mode. To return to the default, use the **no** form of this command.

ip urlfilter max-resp-pak *number* [**vrf** *vrf-name*]

no ip urlfilter max-resp-pak *number*

Syntax Description

number	Maximum number of HTTP responses that can be stored in the packet buffer of the firewall. After the maximum number has been reached, the firewall will drop further responses. The default, and absolute maximum, value is 200.
vrf *vrf-name*	(Optional) Sets the maximum number of HTTP responses only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

200 HTTP responses

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

When an HTTP request arrives at a Cisco IOS firewall, the firewall forwards the request to the web server while simultaneously sending a URL look-up request to the vendor server (Websense or N2H2). If the vendor server reply arrives before the HTTP response, the firewall will know whether to permit or block the HTTP response; if the HTTP response arrives before the vendor server reply, the firewall will not know whether to allow or block the response, so the firewall will drop the response until it hears from the vendor server. The **ip urlfilter max-resp-pak** command allows you to configure your firewall to store the HTTP responses in a buffer, which allows your firewall to store a maximum of 200 HTTP responses. Each response will remain in the buffer until an allow or deny message is received from the vendor server. If the vendor server reply allows the URL, the firewall will release the HTTP response from the buffer to the end user; if the vendor server reply denies the URL, the firewall will discard the HTTP response from the buffer and close the connection to both ends.

Examples

The following example shows how to configure your firewall to hold 150 HTTP responses:

```
ip urlfilter max-resp-pak 150
```

ip urlfilter server vendor

To configure a vendor server for URL filtering, use the **ip urlfilter server vendor** command in global configuration mode. To remove a server from your configuration, use the **no** form of this command.

ip urlfilter server vendor {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**outside**] [**vrf** *vrf-name*]

no ip urlfilter server vendor {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**outside**]

Syntax Description

websense	Websense server will be used.
n2h2	N2H2 server will be used.
ip-address	IP address of the vendor server.
port *port-number*	(Optional) Port number that the vendor server listens on. The default port number is 15868.
timeout *seconds*	(Optional) Length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The default timeout is 5 seconds.
retransmit *number*	(Optional) Number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The default value is two times.
outside	(Optional) Vendor server will be deployed on the outside network.
vrf *vrf-name*	(Optional) Configures a vendor server for URL filtering only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

A vendor server is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	The **outside** keyword was added.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter server vendor** command to configure a Websense or N2H2 server, which will interact with the Cisco IOS Firewall to filter HTTP requests on the basis of a specified policy—global filtering, user- or group-based filtering, keyword-based filtering, category-based filtering, or customized filtering.

If the firewall has not received a response from the vendor server within the time specified in the **timeout** *seconds* keyword and argument, the firewall will check the **retransmit** *number* keyword and argument configured for the vendor server. If the firewall *has not* exceeded the maximum retransmit tries allowed, it will resend the HTTP lookup request. If the firewall *has* exceeded the maximum retransmit tries allowed, it will delete the outstanding request from the queue and check the status of the allow mode value. The firewall will forward the request if the allow mode is on; otherwise, it will drop the request.

By default, URL lookup requests that are made to the vendor server contain non-natted client IP addresses because the vendor server is deployed on the inside network. The **outside** keyword allows the vendor server to be deployed on the outside network, thereby, allowing Cisco IOS software to send the natted IP address of the client in the URL lookup request.

Primary and Secondary Servers

When users configure multiple vendor servers, the firewall will use only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system will go to the beginning of the configured servers list and try to activate the first server on the list. If the first server on the list is unavailable, it will try the second server on the list; the system will keep trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it will set a flag indicating that all of the servers are down, and it will enter allow mode.

Examples

The following example shows how to configure the Websense server for URL filtering:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.

ip urlfilter source-interface

To allow the URL filter to specify the interface whose IP address is used as the source IP address while a TCP connection is made to the URL filter server (Websense or N2H2), use the **ip urlfilter source-interface** command in global configuration mode. To disable the option, use the **no** form of this command.

ip urlfilter source-interface *interface-type* [**vrf** *vrf-name*]

no ip urlfilter source-interface [**vrf** *vrf-name*]

Syntax Description

interface-type	The interface type that is used as the source IP address.
vrf *vrf-name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.

Command Default

The URL filter to specify a source interface for TCP is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **ip urlfilter source-interface** command is used to define the source interface from which the URL filter request is sent. This command is recommended to be configured if the URL filter server can only be routed through certain interfaces on the router.

Examples

The following example shows that the URL filtering server is routed to the Ethernet interface type:

```
Router(config)# ip urlfilter source-interface ethernet
```

Related Commands

Command	Description
debug ip urlfilter	Enables debug information of URL filter subsystems.

ip urlfilter truncate

To allow the URL filter to truncate long URLs to the server, use the **ip urlfilter truncate** command in global configuration mode. To disable the truncating option, use the **no** form of this command.

ip urlfilter truncate {**script-parameters** | **hostname**} [**vrf** *vrf-name*]

no ip urlfilter truncate {**script-parameters** | **hostname**} [**vrf** *vrf-name*]

Syntax Description

script-parameters	Specifies that only the URL up to the script options is sent. • For example, if the entire URL is http://www.cisco.com/dev/xxx.cgi?when=now, only the URL through http://www.cisco.com/dev/xxx.cgi is sent (if the maximum supported URL length is not exceeded).
hostname	Specifies that only the hostname is sent. • For example, if the entire URL is http://www.cisco.com/dev/xxx.cgi?when=now, only http://www.cisco.com is sent.
vrf *vrf-name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.

Command Default

URLs that are longer than the maximum supported length are not truncated, and the HTTP request is rejected.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If both the **script-parameters** and **hostname** keywords are configured, the **script-parameters** keyword takes precedence over the **hostname** keyword. If both the keywords are configured and the script parameters URL is truncated and the maximum supported URL length is exceeded, the URL is truncated up to the hostname.

Note If both **script-parameters** and **hostname** keywords are configured, they must be on separate lines as shown in the "Examples" section. They cannot be combined in one line.

Examples

The following example shows that the URL is to be truncated up to the script options:

```
ip urlfilter truncate script-parameters
```

The following example shows that the URL is to be truncated up to the hostname:

```
ip urlfilter truncate hostname
```

Related Commands

Command	Description
debug ip urlfilter	Enables debug information of URL filter subsystems.

ip urlfilter urlf-server-log

To enable the logging of system messages on the URL filtering server, use the **ip urlfilter urlf-server-log** command in global configuration mode. To disable the logging of system messages, use the **no** form of this command.

ip urlfilter urlf-server-log [**vrf** *vrf-name*]

no ip urlfilter urlf-server-log

Syntax Description

vrf *vrf-name*	(Optional) Enables the logging of system messages on the URL filtering server only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter urlf-server-log** command to enable Cisco IOS to send a log request immediately after the URL lookup request. The firewall will not make a URL lookup request if the destination IP address is in the cache, but it will still make a log request to the server. (The log request contains the URL, hostname, source IP address, and the destination IP address.) The server records the log request into its own log server so your can view this information as necessary.

Examples

The following example shows how to enable system message logging on the URL filter server:

```
ip urlfilter urlf-server-log
```

ip verify drop-rate compute interval

To configure the interval of time between Unicast Reverse Path Forwarding (RPF) drop rate computations, use the **ip verify drop-rate compute interval** command in global configuration mode. To reset the interval to the default value, use the **no** form of this command.

ip verify drop-rate compute interval *seconds*

no ip verify drop-rate compute interval

Syntax Description

seconds	Interval, in seconds, between Unicast RPF drop rate computations. The range is from 30 to 300. The default is 30.

Command Default

The drop rate is not computed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value for the compute interval must be less than or equal to the value configured using the **ip verify drop-rate compute window** command. If you configure the **no** form of the **ip verify drop-rate compute interval** command while the cipUrpfDropRateWindow value is configured to be less than the default compute interval value, the following message appears on the console:

```
"urpf drop rate window < interval"
```

This error message means the command was not executed. The compute interval remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute interval of 45 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute interval 45
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify drop-rate compute window

To configure the interval of time during which the Unicast Reverse Path Forwarding (RPF) drop count is collected for the drop rate computation, use the **ip verify drop-rate compute window** command in global configuration mode. To reset the window to the default value, use the **no** form of this command.

ip verify drop-rate compute window *seconds*

no ip verify drop-rate compute window

Syntax Description

seconds	Interval, in seconds, during which the Unicast RPF drop count is accumulated for the drop rate computation. The range is from 30 to 300. The default is 300.

Command Default

The drop rate is not calculated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

This command configures the sliding window that begins the configured number of seconds prior to the computation and ends with the Unicast RPF drop rate computation. The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value configured for the “compute window” must be greater than or equal to the value configured using the **ip verify drop-rate compute interval** command. If you configure the **no** form of the **ip verify drop-rate compute window** command while the cipUrpfDropRateInterval value is configured to be greater than the default compute window value, the following message appears on the console:

```
“urpf drop rate window < interval”
```

This error message means that the command was not executed. The compute window remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute window of 60 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval between Unicast RPF drop rate computations.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify drop-rate notify hold-down

To configure the minimum time between Unicast Reverse Path Forwarding (RPF) drop rate notifications, use the **ip verify drop-rate notify hold-down** command in global configuration mode. To reset the hold-down time to the default value, use the **no** form of this command.

ip verify drop-rate notify hold-down *seconds*

no ip verify drop-rate notify hold-down

Syntax Description

seconds	Minimum time, in seconds, between Unicast RPF drop rate notifications. The range is from 30 to 300. The default is 300.

Command Default

No notifications are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

Examples

The following example shows how to configure a notify hold-down time of 40 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate notify hold-down 40
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between Unicast RPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time over which the Unicast RPF drop count used in the drop rate computation is collected.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify unicast notification threshold

To configure the threshold value used to determine whether to send a Unicast Reverse Path Forwarding (RPF) drop rate notification, use the **ip verify unicast notification threshold** command in interface configuration mode. To set the notification threshold back to the default value, use the **no** form of this command.

ip verify unicast notification threshold *rate-val*

no ip verify unicast notification threshold

Syntax Description

rate-val	Threshold value, in packets per second, used to determine whether to send a Unicast RPF drop rate notification. The range is from 0 to 4294967295. The default is 1000.

Command Default

No notifications are sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

This command configures the threshold Unicast RPF drop rate which, when exceeded, triggers a notification. Configuring a value of 0 means that any Unicast RPF packet drop triggers a notification.

Examples

The following example shows how to configure a notification threshold value of 900 on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 900
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between Unicast RPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.

ip verify unicast reverse-path

Note This command was replaced by the **ip verify unicast source reachable-via** command effective with Cisco IOS Release 12.0(15)S. The **ip verify unicast source reachable-via** command allows for more flexibility and functionality, such as supporting asymmetric routing, and should be used for any Reverse Path Forward implementation. The **ip verify unicast reverse-path** command is still supported.

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast reverse-path [*list*]

no ip verify unicast reverse-path [*list*]

Syntax Description

list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration mode (config-if)

CommandHistory

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3
12.1(2)T	Added ACL support using the *list* argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	The **ip verify unicast source reachable-via** command replaced this command, and the following keywords were added to the **ip verify unicast source reachable-via** command: **allow-default, allow-self-ping**, **rx**, and **any**.
12.1(8a)E	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(14)SX	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SRA	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip verify unicast reverse-path interface** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that are received by a router. Malformed or forged source addresses can indicate denial of service (DoS) attacks on the basis of source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to ensure that the source address appears in the Forwarding Information Base (FIB) and that it matches the interface on which the packet was received. This "look backwards" ability is available only when Cisco Express Forwarding (CEF) is enabled on the router because the lookup relies on the presence of the FIB. CEF generates the FIB as part of its operation.

To use Unicast RPF, enable CEF switching or distributed CEF (dCEF) switching in the router. There is no need to configure the input interface for CEF switching. As long as CEF is running on the router, individual interfaces can be configured with other switching modes.

Note It is very important for CEF to be configured globally in the router. Unicast RPF will not work without CEF.

Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the CEF table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Where to Use RPF in Your Network

Unicast RPF may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF may also be used in cases for which a router has multiple paths to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an

Internet Service Provider (ISP) are likely to have symmetrical reverse paths. Unicast RPF may still be applicable in certain multi-homed situations, provided that optional Border Gateway Protocol (BGP) attributes such as weight and local preference are used to achieve symmetric routing.

With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. In this scenario, you should use the new form of the command, **ip verify unicast source reachable-via**, if there is a chance of asymmetrical routing.

Examples

The following example shows that the Unicast Reverse Path Forwarding feature has been enabled on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 192.168.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 192.168.200.225 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.255
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny   ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*list*] [**12-src**] [**phys-if**]

no ip verify unicast source reachable-via

Syntax Description

rx	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).
any	Examines incoming packets to determine whether the source address is in the FIB and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).
allow-default	(Optional) Allows the use of the default route for RPF verification.
allow-self-ping	(Optional) Allows a router to ping its own interface or interfaces. **Caution** Use caution when enabling the **allow-self-ping** keyword. This keyword opens a denial-of-service (DoS) hole.
list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)
l2-src	(Optional) Enables source IPv4 and source MAC address binding.
phys-if	(Optional) Enables physical input interface verification.

Command Default

Unicast RPF is disabled.

Source IPv4 and source MAC address binding is disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
12.1(2)T	Added access control list (ACL) support using the *list* argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	This command replaced the **ip verify unicast reverse-path** command, and the following keywords were added: **allow-default**, **allow-self-ping**, **rx**, and **any**.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **l2-src** keyword was added to support the source IPv4 and source MAC address binding feature on Cisco 7600 series routers. The **phys-if** keyword was added to support physical input interface verification. Together, both keywords support the Unicast RPF IP and MAC Address Spoof Prevention feature.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

Note It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.

Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to "look backwards" is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

Note If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are “peered” with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.

Caution Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP

are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

Note With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

IP and MAC Address Spoof Prevention on Cisco 7600 Series Routers

In Release 12.2(33)SRC and later, use the **l2-src** keyword to enable source IPv4 and source MAC address binding and the **phys-if** keyword to verify the source IP input interface. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via** command.The **phys-if** keyword can be used on Gigabit virtual interfaces (GVI) interfaces; the **l2-src** keyword can be used on GVI and Ethernet-like interfaces.

If an inbound packet fails either of these security checks, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

Note Neither the **12-src** nor the **phys-if** keywords can be used with the loose uRPF command, **ip verify unicast source reachable-via any** command.

Possible keyword combinations for Unicast PRF include the following:

```
allow-default
allow-self-ping
l2-src
phys-if
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default phys-if
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping phys-if
allow-self-ping <ACL-number>
l2-src phys-if
l2-src <ACL-number>
phys-if <ACL-number>
allow-default allow-self-ping l2-src
allow-default allow-self-ping phys-if
allow-default allow-self-ping <ACL-number>
allow-default l2-src phys-if
allow-default l2-src <ACL-number>
allow-default phys-if <ACL-number>
allow-self-ping l2-src phys-if
allow-self-ping l2-src <ACL-number>
```

```
allow-self-ping phys-if <ACL-number>
l2-src phys-if <ACL-number>
allow-default allow-self-ping l2-src phys-if
allow-default allow-self-ping l2-src <ACL-number>
allow-default allow-self-ping phys-if <ACL-number>
allow-default l2-src phys-if <ACL-number>
allow-self-ping l2-src phys-if <ACL-number>
allow-default allow-self-ping l2-src phys-if <ACL-number>
```

Examples

Single-homed ISP Connection with Unicast RPF

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or "ip cef distributed" for Route Switch Processor+Versatile Interface Processor-
(RSP+VIP-) based routers.
!
interface Serial5/0/0
 description - link to upstream ISP (single-homed)
 ip address 192.168.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcasts
 no ip proxy-arp
 ip verify unicast source reachable-via
```

ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast source reachable-via rx 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

MAC Address Binding on Cisco 7600 Series Routers

The following example enables source IPv4 and source MAC address binding on VLAN 10.

```
Router# configure terminal
Router(config)# interface VLAN 10
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx l2-src
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.

ip virtual-reassembly

To enable virtual fragment reassembly (VFR) on an interface, use the **ip virtual-reassembly** command in interface configuration mode. To disable VFR on an interface, use the **no** form of this command.

ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

no ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

Syntax Description

max-reassemblies *number*	(Optional) Maximum number of IP datagrams that can be reassembled at any given time. Default value: 16. If the maximum value is reached, all fragments within the following fragment set will be dropped and an alert message will be logged to the syslog server.
max-fragments *number*	(Optional) Maximum number of fragments that are allowed per IP datagram (fragment set). Default value: 32. If an IP datagram that is being reassembled receives more than the maximum allowed fragments, the IP datagram will be dropped and an alert message will be logged to the syslog server.
timeout *seconds*	(Optional) Timeout value, in seconds, for an IP datagram that is being reassembled. Default value: 3 seconds. If an IP datagram does not receive all of the fragments within the specified time, the IP datagram (and all of its fragments) will be dropped.
drop-fragments	(Optional) Enables the VFR to drop all fragments that arrive on the configured interface. By default, this function is disabled.

Defaults

VFR is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

A buffer overflow attack can occur when an attacker continuously sends a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

The **max-reassemblies** *number* option and the **max-fragments** *number* option allow you to configure maximum threshold values to avoid a buffer overflow attack and to control memory usage.

In addition to configuring the maximum threshold values, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time (which can be configured via the **timeout** *seconds* option), the timer will expire and the IP datagram (and all of its fragments) will be dropped.

Automatically Enabling or Disabling VFR

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). Currently, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, VFR will maintain a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled

Examples

The following example shows how to configure VFR on interfaces ethernet2/1, ethernet2/2, and serial3/0 to facilitate the firewall that is enabled in the outbound direction on interface serial3/0. In this example, the firewall rules that specify the list of LAN1 and LAN2 originating protocols (FTP, HTTP and SMTP) are to be inspected.

```
ip inspect name INTERNET-FW ftp
ip inspect name INTERNET-FW http
ip inspect name INTERNET-FW smtp!
!
interface Loopback0
 ip address 10.0.1.1 255.255.255.255
!
interface Ethernet2/0
 ip address 10.4.21.9 255.255.0.0
 no ip proxy-arp
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 description LAN1
 ip address 10.4.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/2
 description LAN2
 ip address 10.15.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 description Internet
 ip unnumbered Loopback0
 encapsulation ppp
 ip access-group 102 in
 ip inspect INTERNET-FW out
 ip virtual-reassembly
 serial restart-delay 0
```

Related Commands

Command	Description
show ip virtual-reassembly	Displays the configuration and statistical information of the VFR on a given interface.

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
ip vrf vpn1
 rd 100:2
 route-target both 100:2
 route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (**interface configuration**)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with a Diameter peer, use the **ip vrf forwarding** command in Diameter peer configuration mode. To enable Diameter peers to use the global (default) routing table, use the **no** form of this command.

ip vrf forwarding *name*

no ip vrf forwarding *name*

Syntax Description

name	Name assigned to a VRF.

Command Default

Diameter peers use the global routing table.

Command Modes

Diameter peer configuration (config-dia-peer)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a Diameter peer. If a VRF name is not configured for a Diameter server, the global routing table will be used.

If the VRF associated with the specified name has not been configured, the command will have no effect and this error message will appear: **No VRF found with the name** *name*.

Examples

The following example shows how to configure the VRF for a Diameter peer:

```
Router (config-dia-peer)# ip vrf forwarding diam_peer_1
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.

ip vrf forwarding (server-group)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) RADIUS or TACACS+ server group, use the **ip vrf forwarding** command in server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

Server groups use the global routing table.

Command Modes

Server-group configuration (server-group)

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(7)T	Functionality was added for TACACS+ servers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA1	This command was integrated into Cisco IOS Release 12.2(33)SRA1.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a AAA RADIUS or TACACS+ server group. This command enables dial users to utilize AAA servers in different routing domains.

Examples

The following example shows how to configure the VRF user to reference the RADIUS server in a different VRF server group:

```
aaa group server radius sg_global
 server-private 172.16.0.0 timeout 5 retransmit 3
!
aaa group server radius sg_water
 server-private 10.10.0.0 timeout 5 retransmit 3 key water
 ip vrf forwarding water
```

The following example shows how to configure the VRF user to reference the TACACS+ server in the server group tacacs1:

```
aaa group server tacacs+tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
server-private	Configures the IP address of the private RADIUS server for the group server.

ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

ip wccp web-cache accelerated [[**group-address** *group-address*] | [**redirect-list** *access-list*] | [**group-list** *access-list*] | [**password** *password*]]

no ip wccp web-cache accelerated

Syntax Description

group-address *group-address*	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the "Usage Guidelines" section for additional information.
redirect-list *access-list*	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the "Usage Guidelines" section for additional information.
group-list *access-list*	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the "Usage Guidelines" section for additional information.
password *password*	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the "Usage Guidelines" section for additional information.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

This command is supported on software releases later than cache engine software Release ACNS 4.2.1.

The **group-address** *group-address* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages

that it has received on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all "Here I Am" messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access-list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access-list number, or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

Related Commands

Command	Description
ip wccp version	Specifies which version of WCCP to configure on your router.

ips signature update cisco

To initiate a one-time download of Cisco IOS Intrusion Prevention System (IPS) signatures from Cisco.com, use the **ips signature update cisco** command in Privileged EXEC mode.

ips signature update cisco {**next** | **latest** | *signature*} [**username** *name* **password** *password*]

Syntax Description

next	Specifies the next signature file version from the current signature file on the router.
latest	Specifies the IOS IPS to search for the latest signature file.
signature	This argument specifies a specific signature file on Cisco.com.
username *name*	Defines the username for the automatic signature update function.
password *password*	Defines the password for the automatic signature update function.

Defaults

Privileged EXEC mode (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The **ips signature update cisco** command is used to initiate a one-time download of IPS signatures from Cisco.com. If you want IPS signatures to be periodically downloaded from Cisco.com, use the **ip ips auto-update** command in global configuration mode and subsequently the **cisco** command in IPS-auto-update configuration mode to enable automatic signature updates from Cisco.com.

If the *username* and *password* is not specified, then the username and password that is specified in the IPS auto update configuration is used. A user name and password must be configured for updating signatures directly from Cisco.com.

Examples

The following example shows how to get the latest automatic signature update from Cisco.com:

```
Router# ips signature update cisco latest
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
cisco	Enables automatic signature updates from Cisco.com.

ipv4 (ldap)

To create an IPv4 address within a Lightweight Directory Access Protocol (LDAP) server address pool, use the **ipv4** command in LDAP server configuration mode. To delete an IPv4 address within an LDAP server address pool, use the **no** form of this command.

ipv4 *ipv4-address*

no ipv4 *ipv4-address*

Syntax Description

ipv4-address	IPv4 address of the LDAP server.

Command Default

No IPv4 addresses are created in the LDAP server address pool.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to create an IPv4 address in an LDAP server address pool:

```
Router(config)# ldap server server1
Router(config-ldap-server)# ipv4 10.0.0.1
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

ipv6 crypto map

To enable an IPv6 crypto map on an interface, use the **ipv6 crypto map** command in interface configuration mode. To disable, use the **no** form of this command.

ipv6 crypto map *map-name*

no ipv6 crypto map

Syntax Description

map-name	Identifies the crypto map set.

Command Default

No IPv6 crypto maps are enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

This command differentiates IPv6 and IPv4 crypto maps.

Examples

The following example shows how to enable an IPv6 crypto map on an interface:

```
Router# configure terminal
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 crypto map CM_V4
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry.

isakmp authorization list

To configure an Internet Key Exchange (IKE) shared secret using the authentication, authorization, and accounting (AAA) server in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **isakmp authorization list** command in ISAKMP profile configuration mode. To disable the shared secret, use the **no** form of this command.

isakmp authorization list *list-name*

no isakmp authorization list *list-name*

Syntax Description

list-name	AAA authorization list used for configuration mode attributes or preshared keys for aggressive mode.

Defaults

No default behaviors or values

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command allows you to retrieve a shared secret from an AAA server.

Examples

The following example shows that an IKE shared secret is configured using an AAA server on a router:

```
crypto isakmp profile vpnprofile
 isakmp authorization list ikessaaalist
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

issuer-name

To specify the distinguished name (DN) as the certification authority (CA) issuer name for the certificate server, use the **issuer-name** command in certificate server configuration mode. To clear the issuer name and return to the default, use the **no** form of this command.

issuer-name *DN-string*

no issuer-name *DN-string*

Syntax Description

DN-string	Name of the DN string.

Defaults

If the issuer name is not configured, **CN** = *cs-label*

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The DN-string value cannot be changed after the certificate server generates its signed certificate.

Examples

The following example shows how to define an issuer name for the certificate server "mycertserver":

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# database level minimal
Router(cs-server)# database url nvram:
Router(cs-server)# issuer-name CN = ipsec_cs,L = My Town,C = US
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

ivrf

To specify a user-defined VPN routing and forwarding (VRF) or use the global VRF, use the **ivrf** command in IKEv2 profile configuration mode. To delete the VRF specification, use the **no** form of this command.

ivrf *name*

no ivrf

Syntax Description

name	VRF name.

Command Default

VRF is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify a user-defined VRF or a global VRF, which should be attached to static and dynamic crypto maps. The inside VRF (IVRF) for a tunnel interface should be configured on the tunnel interface. IVRF specifies the VRF for cleartext packets. The default value for IVRF is Forward VRF (FVRF).

Examples

The following example shows how to specify IVRF:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# ivrf vrf1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show crypto ikev2 profile	Displays the IKEv2 profile.