idle (SSG-radius-proxy-timers)

Note Effective with Cisco IOS Release 15.0(1)M, the **idle** (SSG-radius-proxy-timers) command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) host object timeout value, use the **idle** command in SSG-radius-proxy-timers configuration mode. To disable the timeout value, use the **no** form of this command.

idle *timeout*

no idle *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 30 to 65536 seconds. There is no default value.

Command Default

No idle timeout value is configured.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced to replace the **idle-timeout** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an idle timeout value for a host object. Configuring this command prevents dangling host objects on SSG. If a RADIUS client reloads and does not indicate its fault condition to SSG, SSG retains host objects that are no longer valid. This command removes all host objects from a RADIUS client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.

Note Timeout values configured in the user profile that appears in the Access-Accept packet take precedence over any timeout value configured by the **timeouts** (SSG-radius-proxy) command.

Note This command replaces the **idle-timeout** command in SSG-radius-proxy configuration mode.

Examples

The following example shows how to configure an idle timeout value of 60 seconds:

```
ssg radius-proxy
 ssg timeouts
 idle 60
```

Related Commands

Command	Description
hand-off	Configures an SSG RADIUS proxy handoff timeout.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

idle-timeout (SSG)

Note Effective with Cisco IOS Release 15.0(1)M, the **idle-timeout** (SSG) command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command was replaced by the **idle** (SSG radius-proxy-timers) command. The **idle-timeout** command is still supported for backward compatibility, but support for this command may be removed in a future Cisco IOS release.

To configure a host object timeout value, use the **idle-timeout** command in SSG-radius-proxy configuration mode. To disable the timeout value, use the **no** form of this command.

idle-timeout *timeout*

no idle-timeout *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is from 30 to 65536.

Command Default

No timeout value is configured.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **idle** (SSG radius-proxy-timers) command.
12.3(4)T	This command was replaced by the **idle** (SSG radius-proxy-timers) command.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure a timeout value for a host object. Configuring this command prevents dangling host objects on the Service Selection Gateway (SSG). If a RADIUS client reloads and does not indicate its fault condition to the SSG, the SSG retains the host objects that are no longer valid. This command removes all host objects from a RADIUS client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.

Note Timeout values configured in the user profile that appear in the Access-Accept take precedence over any timeout value configured by the **idle-timeout** command.

Examples

The following example shows how to configure a timeout value of 60 seconds:

```
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 10.1.2.2 key secret1
 client-address 10.2.25.90 key secret2
 client-address 10.0.0.1 key secret3
 client-address 10.23.3.2 key secret4
 idle-timeout 60
 forward accounting-start-stop
 address-pool 10.1.1.1 10.1.40.250
 address-pool 10.1.5.1 10.1.5.30 domain ssg.com
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

ip-address (SSG-radius-proxy-timers)

Note Effective with Cisco IOS Release 15.0(1)M, the **ip-address** (SSG-radius-proxy-timers) command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) RADIUS proxy IP address timeout, use the **ip-address** command in SSG-radius-proxy-timers configuration mode. To disable the IP address timeout, use the **no** form of this command.

ip-address *timeout*

no ip-address *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 1 to 30 seconds. The default is 5 seconds.

Command Default

The default value of this timeout is 5 seconds.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an SSG RADIUS proxy IP address timeout.

If SSG, acting as a RADIUS proxy for a client, does not allocate an IP address in the Access-Accept packet, a dormant host object is created. The dormant host object is not activated until SSG receives an Accounting-Start packet from the client device, containing a valid IP address.

When an IP address timeout is configured, SSG starts this timer on creation of the dormant host object. If a valid IP address is not received via an Accounting-Start packet from the client device, prior to the expiration of this timeout, the dormant host object is destroyed.

Examples

The following example shows how to configure an SSG RADIUS proxy IP address timeout of 10 seconds:

```
ssg radius-proxy
 ssg timeouts
 ip-address 10
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
hand-off	Configures an SSG RADIUS proxy handoff timeout.
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

key (SSG-radius-proxy-client)

Note Effective with Cisco IOS Release 15.0(1)M, the **key** (SSG-radius-proxy-client) command is not available in Cisco IOS software.

To configure a shared secret between the Service Selection Gateway (SSG) and a RADIUS client, use the **key** command in SSG-radius-proxy-client mode. To unconfigure the shared secret, use the **no** form of this command.

key *secret*

no key *secret*

Syntax Description

secret	Description of the shared secret.

Command Default

No default behavior or values.

Command Modes

SSG-radius-proxy-client

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure a shared secret between SSG and a RADIUS client. Use the *secret* attribute to configure each client IP with a unique shared secret. This shared secret should be the same one that is configured on the RADIUS client.

Note The **key** command in SSG-radius-proxy-client mode replaces the **client-address key** command in SSG-radius-proxy mode.

Examples

The following example shows how to configure the RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server and assigns the shared secret “cisco” to the client:

```
client-address 172.16.0.0
 key cisco
```

Related Commands

Command	Description
client-address	Configures the RADIUS client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-client mode.

length (SSG)

Note Effective with Cisco IOS Release 15.0(1)M, the **length** (SSG) command is not available in Cisco IOS software.

To modify the port-bundle length upon the next Service Selection Gateway (SSG) reload, use the **length** command in SSG portmap configuration mode. To return the port-bundle length to the default value, use the **no** form of this command.

length *bits*

no length *bits*

Syntax Description

bits	Port-bundle length, in bits. The range is from 0 to 10 bits. The default is 4 bits.

Command Default

4 bits.

Command Modes

SSG portmap configuration

Command History

Release	Modification
12.2(16)B	This command was introduced. This command replaces the **ssg port-map destination range** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The port-bundle length is used to determine the number of bundles in one group and the number of ports in one bundle. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See Table 8 for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. Increasing the port-bundle length can be useful when you see frequent error messages about running out of ports in a port bundle, but note that the new value does not take effect until SSG next reloads and Cisco Service Selection Dashboard (SSD) restarts.

Note For each Cisco SSD server, all connected SSGs must have the same port-bundle length.

Table 8 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per-SSG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

Examples

The following example results in 64 ports per bundle and 1008 bundles per group:

```
ssg port-map
 length 6
```

Related Commands

Command	Description
source ip	Specifies SSG source IP addresses to which to map the destination IP addresses in subscriber traffic.
ssg port-map	Enables the SSG port-bundle host key and enters SSG portmap configuration mode.

local-profile

Note Effective with Cisco IOS Release 15.0(1)M, the **local-profile** command is not available in Cisco IOS software.

To configure a local service profile and enter profile configuration mode, use the **local-profile** command in global configuration mode. To delete the local service profile, use the **no** form of this command.

local-profile *profile-name*

no local-profile *profile-name*

Syntax Description

profile-name	Name of profile to be configured.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 series node route processor.
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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure local service profiles.

Examples

The following example shows how to configure a RADIUS profile called “fictitiousname.com” and enter profile configuration mode:

```
Router(config)# local-profile fictitiousname.com
Router(config-prof)#
```

In the following example, two services called “og1” and “og2” are defined and added to the open garden:

```
!
ssg open-garden og1
ssg open-garden og2
!
local-profile og1
 attribute 26 9 251 "Oopengarden1.com"
 attribute 26 9 251 "D10.13.1.5"
```

```
 attribute 26 9 251 "R10.1.1.0;255.255.255.0"
local-profile og2
 attribute 26 9 251 "Oopengarden2.com"
 attribute 26 9 251 "D10.14.1.5"
 attribute 26 9 251 "R10.2.1.0;255.255.255.0"
 attribute 26 9 251 "R10.3.1.0;255.255.255.0"
!
ssg bind service og2 10.5.5.1
```

Related Commands

Command	Description
attribute	Configures attributes in local RADIUS profiles.
show ssg open-garden	Displays a list of all configured open garden services.
ssg open-garden	Designates a service, defined in a local service profile, as an open garden service.
ssg service-search-order	Specifies the order in which SSG searches for a service profile.

max-sessions host

Note Effective with Cisco IOS Release 15.0(1)M, the **max-sessions host** command is not available in Cisco IOS software.

To set the maximum number of TCP sessions that can be established by an unauthenticated host, use the **max-sessions host** command in SSG TCP-redirect server-group configuration mode. To remove this setting, use the **no** form of this command.

max-sessions host *number-of-sessions*

no max-sessions host *number-of-sessions*

Syntax Description

number-of-sessions	Maximum number of TCP sessions per unauthenticated host. The range is from 1 to 65535.

Command Default

No limit on the number of TCP sessions that can be established by an unauthenticated host.

Command Modes

SSG TCP-redirect server-group configuration

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **max-sessions host** command to configure a per-host limit on the number of TCP sessions that can be established by unauthenticated hosts that are redirected to the server group.

The maximum number of TCP connections allowed per host, as configured by the **max-sessions host** command, should be greater than the average number of TCP connections required when a page is accessed.

Examples

The following example sets the maximum number of TCP sessions that can be established by an unauthenticated host at 20 sessions:

```
ssg tcp-redirect
 server-group test_group
  Server 10.10.10.1 90
  max-sessions host 20
```

Related Commands

Command	Description
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG TCP-redirect server-group configuration mode.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG TCP-redirect configuration mode.

mode extended

Note Effective with Cisco IOS Release 15.0(1)M, the **mode extended** command is not available in Cisco IOS software.

To select extended Autodomain mode, use the **mode extended** command in SSG-auto-domain configuration mode. To reenable basic Autodomain mode, use the **no** form of this command.

mode extended

no mode extended

Syntax Description

This command has no arguments or keywords.

Command Default

Basic Autodomain mode is selected.

Command Modes

SSG-auto-domain configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **mode extended** command to select the extended Autodomain mode. In basic Autodomain mode, the profile downloaded from the AAA server for the selected Autodomain name is a service profile, which may or may not contain attributes specific to Service Selection Gateway (SSG). In extended Autodomain mode, the profile is a "virtual user" profile, which may contain a list of services in addition to other account attributes. The "virtual user" profile contains one autoservice to an authenticated service such as a proxy, VPDN, or tunnel. Connection to the autoservice occurs in the same way as in basic Autodomain mode. The host object is not activated until the user is authenticated at the service. The presence of SSD allows the user to access any other service in the specified user profile. Extended mode also enables users with multiple service selection to log on.

Examples

The following example shows how to enable extended Autodomain mode:

```
ssg enable
ssg auto-domain
 mode extended
 select username
 exclude apn company
 exclude domain cisco
 download exclude-profile abc password1
 nat user-address
```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
nat user-address	Enables NAT on Autodomain tunnel service.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg auto-domain	Enables SSG Autodomain mode.
ssg enable	Enables SSG functionality.

msid (SSG-radius-proxy-timers)

Note Effective with Cisco IOS Release 15.0(1)M, the **msid** (SSG-radius-proxy-timers) command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) RADIUS proxy mobile station ID (MSID) timeout, use the **msid** command in SSG-radius-proxy-timers configuration mode. To disable the MSID timeout, use the **no** form of this command.

msid *timeout* **retry** *retries*

no msid *timeout* **retry** *number-of-retries*

Syntax Description

timeout	Timeout value in seconds. Valid range is 1 to 5 seconds. The default is 1 second.
retry *number-of-retries*	Maximum number of retries. Valid range is 1 to 20 retries. The default is 10 retries.

Command Default

The default value of this timeout is 1 second, with a default retry count of 10.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an MSID timeout.

Configure the MSID timer to associate an MSID to the host object for a Mobile IP connection. The MSID is associated with a host object only after SSG receives the Accounting-Start packets from the Packet Data Serving Node (PDSN)/Foreign Agent (FA) and the Home Agent (HA). The host object address is not assigned until SSG receives the Accounting-Start packet from the HA. If the Accounting-Start packet from the PDSN/FA arrives before the Accounting-Start packet from the HA, the host object cannot be located, and the MSID is not associated with the host object. When this occurs, the retry timer is started. When the retry timer expires, the MSID is associated with the host object.

If SSG does not receive the Account-Start packet with the correct MSID from the PDSN before the timeout expires, the host object is removed.

Examples

The following example shows how to configure an SSG RADIUS proxy MSID timeout of 3 seconds with 5 retries:

```
ssg radius-proxy
 timeouts
 msid 3 retry 5
```

Related Commands

Command	Description
hand-off	Configures an SSG RADIUS proxy hand off timeout.
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

nat user-address

Note Effective with Cisco IOS Release 15.0(1)M, the **nat user-address** command is not available in Cisco IOS software.

To enable Network Address Translation (NAT) toward Autodomain service, use the **nat user-address** command in SSG-auto-domain mode. To disable NAT on Autodomain service, use the **no** form of this command.

nat user-address

no nat user-address

Syntax Description

This command has no arguments or keywords.

Command Default

NAT is not applied toward Autodomain services and IP addresses assigned at the tunnel, VPDN, or proxy service will be assigned at the host and then sent back to the RADIUS client. NAT is always applied towards the Autodomain connection regardless of the configuration of the **nat user-address** command when the Access-Request from the RADIUS client contains an IP address.

Command Modes

SSG-auto-domain

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **nat user-address** command to enable NAT toward the Autodomain connection. When a host object has not been assigned an IP address using the Access-Request from the RADIUS client, Service Selection Gateway (SSG) by default passes an IP address assigned at the tunnel, VPDN, or proxy service back to the RADIUS client and NAT does not happen toward the Autodomain connection. The **nat user-address** command overrides the default behavior and specifies that NAT should be performed towards Autodomain services. If a host has been assigned an IP address via the Access-Request, NAT happens toward the Autodomain connection regardless of the status of this command.

Examples

The following example enables NAT toward the Autodomain connection:

```
ssg enable
ssg auto-domain
 mode extended
 select username
```

```
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address
```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

network (ssg-redirect)

Note Effective with Cisco IOS Release 15.0(1)M, the **network** (ssg-redirect) command is not available in Cisco IOS software.

To add an IP address to a named network list, use the **network** command in SSG-redirect-network configuration mode. To remove an IP address from a named network list, use the **no** form of this command.

network *ip-address mask*

no network *ip-address mask*

Syntax Description

ip-address	IP address that is to be added to a named network list.
mask	Mask for the associated IP subnet.

Command Default

No default behavior or values

Command Modes

SSG-redirect-network configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to define an individual network that is found in a named network list. Use the **network-list** command to define and name the network list and the **network** command to add an individual IP address to the named network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example creates a network list named "RedirectNw" and adds IP address 10.0.0.0 255.0.0.0 and address 10.2.2.0 255.255.255.0 to the "RedirectNw" network list:

```
ssg tcp-redirect
 network-list RedirectNw
  network 10.0.0.0 255.0.0.0
  network 10.2.2.0 255.255.255.0
```

Related Commands

Command	Description
network-list	Defines a list of one or more IP networks that make up a named network list.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

network-list

Note Effective with Cisco IOS Release 15.0(1)M, the **network-list** command is not available in Cisco IOS software.

To define a list of one or more IP networks that make up a named network list and to enter SSG-redirect-network configuration mode, use the **network-list** command in SSG-redirect configuration mode. To remove a named network list, use the **no** form of this command.

network-list *network-listname*

no network-list *network-listname*

Syntax Description

network-listname	Defines the name of the network list.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to define a list of one or more IP networks that make up a named network list. Use the *network-listname* attribute to name the IP network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example defines an IP network list named “RedirectNw”:

```
network-list RedirectNw
```

Related Commands

Command	Description
network (ssg-redirect)	Adds an IP address to a named network list.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

port (ssg-redirect)

Note Effective with Cisco IOS Release 15.0(1)M, the **port** (ssg-redirect) command is not available in Cisco IOS software.

To add a TCP port to a named port list, use the **port** command in SSG-redirect-port configuration mode. To remove a TCP port from a named port list, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Incoming destination port number.

Command Default

No default behavior or values.

Command Modes

SSG-redirect-port configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to add incoming destination ports to a named TCP port list. Incoming packets directed to a port in the named TCP port list can be redirected by the named captive portal group. Configure the named captive portal group using the **server-group** command, and add servers to the captive portal group using the **server** (SSG) command. Define and name the TCP port list using the **port-list** command.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define or add incoming destination ports to a named TCP port list.

Examples

The following example creates a named TCP port list named “WebPorts” and adds TCP ports 80 and 8080:

```
ssg enable
 ssg tcp-redirect
  port-list WebPorts
   port 80
   port 8080
```

Related Commands

Command	Description
port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

port-list

Note Effective with Cisco IOS Release 15.0(1)M, the **port-list** command is not available in Cisco IOS software.

To define a list of one or more TCP ports that make up a named port list and to enter SSG-redirect-port configuration mode, use the **port-list** command in SSG-redirect configuration mode. To disable a port list, use the **no** form of this command.

port-list *port-listname*

no port-list *port-listname*

Syntax Description

port-listname	Defines the name of the port list.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to define a named port list. Use this command to create a list of TCP ports that can be redirected by the captive portal group. Use the **port** (ssg-redirect) command in SSG-redirect-port configuration mode to add TCP ports to the named port list.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named port list.

Examples

The following example creates a port list named “WebPorts”:

```
ssg enable
 ssg tcp-redirect
  port-list WebPorts
```

Related Commands

Command	Description
port (ssg-redirect)	Adds a TCP port to a named port list.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

query ip dhcp

Note Effective with Cisco IOS Release 15.0(1)M, the **query ip dhcp** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to send a Dynamic Host Configuration Protocol (DHCP) lease query request for the subscriber session created under a RADIUS proxy client when no IP address appears in the accounting-start record, use the **query ip dhcp** command in the client-address submode of SSG-radius-proxy mode. To disable the sending of the lease query request, use the **no** form of this command.

query ip dhcp

no query ip dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

SSG sends the subscriber's IP address as the username (RADIUS attribute 1).

Command Modes

Client-address submode of SSG-radius-proxy mode

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **query ip dhcp** command to send DHCP lease query requests for a subscriber session under a specified RADIUS proxy client when no IP address is received in the accounting start record.

Examples

The following example enables DHCP lease query requests for RADIUS proxy client 10.0.0.0:

```
ssg enable
 ssg radius-proxy
 client-address 10.0.0.0
 query ip dhcp
```

Related Commands

Command	Description
ssg query mac dhcp	Sends a DHCP lease query request to the DHCP server when a subscriber's MAC address is not known.
username mac	Sends a subscriber's MAC address as RADIUS attribute 1 in TAL requests.

redirect access-list

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect access-list** command is not available in Cisco IOS software.

To associate an access control list with a Service Selection Gateway (SSG) TCP redirect server group, use the **redirect access-list** command in SSG-redirect mode. To remove the association, use the **no** form of this command.

redirect access-list {*number* | *name*} [**to** *groupname*]

no redirect access-list {*number* | *name*} [**to** *groupname*]

Syntax Description

number	Specifies the access control list number.
name	Specifies the access control list name.
to *groupname*	(Optional) Defines the group name of the server group to which the access control list is redirected. If no server group is specified, the access control list is used for redirection to any server group that does not have an access control list associated with it.

Command Default

An access control list is not associated with an SSG TCP redirect server group.

Command Modes

SSG-redirect

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to associate an access control list with a TCP redirect server group. By associating an access control list with a redirect group, you can limit the kind of traffic that is redirected on the basis of the source or destination IP address and TCP ports. It can also be used to redirect different sets of users to different dashboards for unauthenticated users and unauthorized service redirection.

If a port list and an access control list are both associated with a server group, the TCP packet must match the access control list and port list. Only one access control list can be associated with a server group. Either an access control list or a port or port list should be configured with server groups for unauthorized service redirection and captivation.

If a server group is not specified, the access control list is used for redirection to any server group that does not have an access control list associated with it.

The access control list can be a simple or extended access control list. It can also be a named or numbered access control list.

Examples

The following example redirects access control list 101 to server group "InitialCapt":

```
redirect access-list 101 to InitialCapt
```

The following example redirects access control list 50 to server group "SESM1":

```
redirect access-list 50 to SESM1
```

Related Commands

Command	Description
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect captivate advertising default group

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect captivate advertising default group** command is not available in Cisco IOS software.

To configure the default captive portal group, duration, and frequency for advertising captivation, use the **redirect captivate advertising default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for advertising captivation, use the **no** form of this command.

redirect captivate advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

no redirect captivate advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

Syntax Description

group-name	Name of the captive portal group.
duration *seconds*	The duration in seconds of the advertising captivation. The valid range is from 1 to 65536 seconds.
frequency *frequency*	The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is from 1 to 65536 seconds.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to select the default captive portal group for advertising captivation of users upon Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the advertising captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

Use the *frequency* argument to configure how often Service Selection Gateway (SSG) attempts to forward packets from the user to the captive portal.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples

The following example shows how to configure the captive portal group named "CaptivateServer" to forward packets from a user for 30 seconds at intervals of 3600 seconds:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect captivate initial default group

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect captivate initial default group** command is not available in Cisco IOS software.

To select a default captive portal group and duration of the initial captivation of users on Account Logon, use the **redirect captivate initial default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for initial captivation, use the **no** form of this command.

redirect captivate initial default group *group-name* **duration** *seconds*

no redirect captivate initial default group *group-name* **duration** *seconds*

Syntax Description

group-name	Name of the captive portal group.
duration *seconds*	Duration in seconds of the initial captivation. The valid range is from 1 to 65536 seconds.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to select the default captive portal group for initial captivation of users on Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the initial captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples

The following example shows that the captive portal group named “CaptivateServer” will be used to forward packets from a user for the first 10 seconds that the user is connected:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
```

```
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect permanent http to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect permanent http to** command is not available in Cisco IOS software.

To configure Service Selection Gateway (SSG) with permanent TCP redirection for HTTP proxy server support, use the **redirect permanent http to** command in SSG-redirect configuration mode. To disable permanent TCP redirection, use the **no** form of this command.

redirect permanent http {**authenticated** | **unauthenticated**} **to** *server-group*

no redirect permanent http {**authenticated** | **unauthenticated**} **to** *server-group*

Syntax Description

authenticated	Redirects HTTP traffic to the HTTP proxy server for authenticated users.
unauthenticated	Redirects HTTP traffic to the HTTP proxy server for unauthenticated users.
server-group	Server group name to which HTTP traffic will be sent.

Command Default

Permanent TCP redirection is not configured.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.3(3)B	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Permanent TCP redirection enables SSG to support users whose web browsers are configured with HTTP proxy servers.

Examples

The following example shows how to configure SSG to support permanent TCP redirection for authenticated and unauthenticated HTTP proxy users:

```
ssg tcp-redirect
 server-group unauthen-group
  server 10.10.86.90 80
 !
 server-group auth_web_group
  server 10.10.36.253 80
!
 server-group unauth_web_group
  server 10.10.76.12 80
```

```
!
redirect unauthenticated-user to unauthen-group
!
redirect permanent http unauthenticated to unauth_web_group
!
redirect permanent http authenticated to auth_web_group
```

Related Commands

Command	Description
server	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group.
show ssg host	Displays information about a subscriber and current connections of the subscriber.
show ssg tcp-redirect mapping	Displays information about the TCP redirect mappings for hosts within your system.

redirect prepaid-user to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect prepaid-user to** command is not available in Cisco IOS software.

To configure a captive portal group for redirection of prepaid user traffic, use the **redirect prepaid-user to** command in SSG-redirect configuration mode. To configure SSG not to redirect prepaid users to the specified captive portal group, use the **no** form of this command.

redirect prepaid-user to *group-name*

no redirect prepaid-user to *group-name*

Syntax Description

group-name	Name of the captive portal group

Command Default

If no redirect group is configured, prepaid traffic is dropped.

Command Modes

SSG-redirect

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure and name a captive portal group to which prepaid user traffic is redirected. When a user that is logged on to a prepaid service runs out of quota on the billing server, the user is redirected to the configured captive portal group if the service is not configured with any specific redirect server group. Once redirected to the captive portal group, the user can refill the quota on the billing server without being disconnected from the original prepaid service.

The captive portal group is the default group for all services that are not configured with a redirect group.

Examples

The following example shows how to configure a captive portal group called “DefaultRedirectGroup”, add two servers to “DefaultRedirectGroup”, and redirect prepaid users to the newly created captive portal:

```
ssg enable
ssg tcp-redirect
 server-group DefaultRedirectGroup
  server 10.0.0.1 8080
```

```
 server 10.0.0.20 80
 end
redirect prepaid-user to DefaultRedirectGroup
```

Related Commands

Command	Description
server	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect smtp group

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect smtp group** command is not available in Cisco IOS software.

To select a captive portal group for redirection of Simple Mail Transfer Protocol (SMTP) traffic, use the **redirect smtp group** command in SSG-redirect configuration mode. To stop redirecting SMTP traffic to a captive portal group, use the **no** form of this command.

redirect smtp group *group-name* [**all** | **user**]

no redirect smtp group *group-name* [**all** | **user**]

Syntax Description

group-name	Name of the captive portal group.
all	(Optional) Any SMTP packets are forwarded.
user	(Optional) SMTP packets from users that have SMTP forwarding permission are forwarded.

Command Default

SMTP traffic is not forwarded to a captive portal group.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to select a captive portal group for redirection of SMTP traffic. If you select the **all** keyword, all SMTP packets (TCP port 25) from authorized users are redirected to one of the servers in the captive portal group specified by the *group-name* argument. If you select the **user** keyword, only SMTP packets from authorized users that have SMTP forwarding permission set through a RADIUS attribute are redirected. If you do not select a keyword, the default is the **all** keyword.

Examples

The following example shows how to configure all SMTP packets from authorized users to be redirected to the captive portal group named “SMTPServer”:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
```

```
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

The following example shows how to configure SMTP packets from any authorized user with the SMTP forwarding permission set through a RADIUS attribute to be redirected to the captive portal group named "SMTPServer":

```
redirect smtp group SMTPServer user
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect to** command is not available in Cisco IOS software.

To configure a TCP port or named TCP port list for Service Selection Gateway (SSG) TCP Redirect for Services, use the **redirect to** command in SSG-redirect configuration mode. To disable SSG TCP Redirect for Services on a TCP port or named TCP port list, use the **no** form of this command.

redirect {**port-list** *port-listname* | **port** *port-number*} **to** *group-name*

no redirect {**port-list** *port-listname* | **port** *port-number*} **to** *group-name*

Syntax Description

port-list	Specifies the named TCP port list to mark for SSG TCP redirection.
port-listname	Specifies the name of the named TCP port list.
port	Specifies a TCP port to mark for SSG TCP redirection.
port-number	Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
group-name	Defines the name of the captive portal group to redirect packets to that are marked for a destination port or named TCP port list.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to mark a TCP port or a named TCP port list for SSG TCP Redirect for Services. Define a named TCP port list using the **port-list** command and add TCP ports to the named TCP port list using the **port** (ssg-redirect) command. Packets arriving from an authorized user, or from an authorized user attempting to access an unauthorized service at a marked TCP port or named TCP port list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen.

Note You can associate only one port or port list with a portal group.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a TCP port or named TCP port list for SSG TCP redirection.

Note This command replaces the **ssg http-redirect port group** command.

Examples

The following example marks TCP port 8080 for SSG TCP redirection. Packets with a destination port of 8080 are redirected to the captive portal group named "RedirectServer":

```
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 8080 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example marks the named TCP port "WebPorts" for SSG TCP redirection. Packets with a destination port that is one of the ports in the port list "WebPorts" are redirected to the captive portal group named "RedirectServer":

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to RedirectServer
!
```

Related Commands

Command	Description
port (ssg-redirect)	Adds a TCP port to a named port list.
port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect unauthenticated-user to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect unauthenticated-user to** command is not available in Cisco IOS software.

To redirect TCP traffic from unauthenticated users to a specified captive portal group, use the **redirect unauthenticated-user to** command in Service Selection Gateway SSG-redirect configuration mode. To stop redirecting traffic from unauthenticated users to the specified captive portal group, use the **no** form of this command.

redirect unauthenticated-user to *group-name*

no redirect unauthenticated-user to *group-name*

Syntax Description

group-name	The name of the captive portal group.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to redirect traffic from unauthenticated users to a specified captive portal group.

Note This command replaces the **ssg http-redirect unauthorized-user group** command.

Examples

The following example sets redirection of traffic from unauthenticated users to the captive portal group named “RedirectServer”:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
```

```
redirect captivate initial default group CaptivateServer duration 10
redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect unauthorized-service service to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect unauthorized-service service to** command is not available in Cisco IOS software.

To redirect traffic that is destined for an unauthorized service to a specified server group, use the **redirect unauthorized-service service to** command in SSG TCP-redirect configuration mode. To remove this redirection, use the **no** form of this command.

redirect unauthorized-service service *service-name* **to** *server-group*

no redirect unauthorized-service service *service-name* **to** *server-group*

Syntax Description

service-name	Name of the unauthorized service.
server-group	Name of the server group to which traffic will be forwarded.

Command Default

Users trying to access a service that they are unauthorized to access will not be redirected.

Command Modes

SSG TCP-redirect configuration

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The **redirect unauthorized-service service to** command causes SSG to download the service profile from the authentication, authorization, and accounting (AAA) server and create mappings for the networks associated with the service. If traffic is received for the specified service while the service profile is being downloaded, the traffic either will be dropped or will be forwarded if Internet service is available to the user.

Examples

In the following example, users who are trying to access the service “test_service” but are unauthorized for that service will be forwarded to the server group “test_group”:

```
ssg tcp-redirect
 Server-group test_group
  Server 10.10.10.1 90
!
!
 Port-list test_ports
  Port 777
```

```
!
!
 redirect port-list test_ports to test_group
!
 redirect unauthorized-service service test_service to test_group
```

Related Commands

Command	Description
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG TCP-redirect configuration mode.

redirect unauthorized-service to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect unauthorized-service to** command is not available in Cisco IOS software.

To set a list of destination IP networks that can be redirected by a specified, named captive portal group, use the **redirect unauthorized-service to** command in SSG-redirect configuration mode. To remove the list of IP networks that can be redirected by a specified named captive portal group, use the **no** form of this command.

redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

no redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

Syntax Description

destination network list	(Optional) Checks incoming packets from authenticated hosts to networks that they are not authorized to access to determine if they need redirection.
network-listname	(Optional) Name of the list of destination IP networks.
group-name	Name of the captive portal group.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to set a list of destination IP networks that can be redirected by the named captive portal group specified by the *group-name* argument. Incoming packets from authenticated hosts to networks that they are not authorized to access are checked against the destination IP network list to determine if they need redirection. If you do not specify a destination IP network by configuring the optional **destination network-list** keywords, the captive portal group specified in the *group-name* argument is used as the default group for unauthorized service redirection when the IP address of the unauthorized packet does not fall into any network list associated with any captive portal group.

You can associate only one destination IP network list with a captive portal group. You can associate a destination IP network list with multiple captive portal groups.

When you associate a destination IP network list with a captive portal group, packets arriving marked with a destination IP network that matches an IP network list may be redirected via SSG TCP redirection. The incoming destination TCP port also determines whether a packet is a candidate for SSG TCP redirection.

You can associate different server groups with overlapping IP network addresses. You must configure the captive portal group associated with a more specific network group first. For example, you must configure

```
redirect 10.1.0.0/255.255.0.0 to IPTVGroup
```

before you can configure

```
redirect 10.0.0.0/255.0.0.0 to ISPGroup
```

Examples

The following example shows how to set the captive portal group called "RedirectServer" as a possible candidate for redirection when the destination of a packet matches one of the networks in the destination IP network list named "RedirectNW":

```
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 80 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example shows how to set the captive portal group called "DefaultRedirectServer" as a possible candidate for redirection when the destination of a packet does not match any of the networks defined in any destination IP network list:

```
redirect unauthorized-service to DefaultRedirectServer
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

remove vsa

Note Effective with Cisco IOS Release 15.0(1)M, the **remove-vsa** command is not available in Cisco IOS software.

To allow all Third Generation Partnership Project 2 (3GPP2) vendor-specific attributes (VSAs) or all Cisco VSAs from Access-Accept packets proxied from a authentication, authorization, and accounting (AAA) server to a RADIUS client to be removed, use the **remove vsa** command in SSG-radius-proxy-client mode. To enable all 3GPP2 VSAs or Cisco VSAs to be passed transparently, use the **no** form of this command.

remove vsa {**3gpp2** | **cisco**}

no remove vsa {**3gpp2** | **cisco**}

Syntax Description

3gpp2	Removes all 3GPP2 VSAs.
cisco	Removes all Cisco VSAs.

Command Default

By default, Service Selection Gateway (SSG) removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. All 3GPP2 VSAs are, by default, passed transparently.

Command Modes

SSG-radius-proxy-client

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to remove all 3GPP2 VSAs or Cisco VSAs from a RADIUS client.

By default, SSG removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. This is because the client device is unlikely to understand the VSAs, and their presence may cause interoperation difficulties. The **no remove vsa cisco** command may be used to allow these attributes to be passed transparently.

You can use this command to remove all 3GPP2 VSAs in addition to Cisco VSAs by using the **3gpp2** keyword. 3GPP2 VSAs are not filtered by default, whereas Cisco VSAs are filtered by default. SSG VSAs (a subset of Cisco VSAs) are always removed, irrespective of any configuration.

Examples

The following example shows how to remove all 3GPP2 VSAs from an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa 3gpp2
```

The following example shows how to transparently pass all Cisco VSAs in an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa cisco
```

Related Commands

Command	Description
client-address	Configures a RADIUS client to proxy requests from the specified IP address to a RADIUS server and enters SSG-radius-proxy-client mode.