



SSG TCP Redirect for Services

Feature History

Release	Modification
12.1(5)DC	This feature was introduced on Cisco 6400 series routers as the HTTP Redirect feature.
12.2(4)B	This feature was integrated into Cisco IOS Release 12.2(4)B.
12.2(16)B	TCP Redirect, Prepaid Server and AAA Groups, Unauthorized Service Redirect based on service name, Interface Binding, and default values for QoS enhancements were added into Cisco IOS Release 12.2(16)B.

This document describes the SSG TCP Redirect for Services feature and contains the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 4](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 5](#)
- [Monitoring and Maintaining SSG TCP Redirect for Services, page 12](#)
- [Configuration Examples, page 13](#)
- [Command Reference, page 16](#)
- [Replaced Commands, page 58](#)
- [Glossary, page 59](#)

Feature Overview

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

The SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

SSG acts as a central control point for Layer 2 and Layer 3 services. This can include services available through Asynchronous Transfer Mode (ATM) virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

SSG communicates with the authentication, authorization, and accounting (AAA) management network where Remote Authentication Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

For more information about SSG, refer to the [Service Selection Gateway](#) feature module. For more information about SESM, refer to the Cisco Subscriber Edge Services Manager documentation.

TCP Redirect for Services

The SSG TCP Redirect for Services feature redirects certain packets, which would otherwise be dropped, to captive portals that can handle the packets in a suitable manner. For example, packets sent upstream by unauthorized users are forwarded to a captive portal that can redirect the users to a logon page. Similarly, if users try to access a service to which they have not logged on, the packets are redirected to a captive portal that can provide a service logon screen.

The captive portal can be any server that is programmed to respond to the redirected packets. If the Cisco Subscriber Edge Services Manager (SESM) is used as a captive portal, unauthenticated subscribers can be sent automatically to the SESM logon page when they start a browser session. In SESM Release 3.1(3), captive portal applications can also redirect to service logon pages, advertising pages, and message pages. The SESM captive portal application can also capture a URL in a subscriber's request and redirect the browser to the originally requested URL after successful authentication. Redirected packets are always sent to a captive portal group that consists of one or more servers. SSG selects one server from the group in a round-robin fashion to receive the redirected packets.

Benefits

SSG TCP Redirect for Services provides the following benefits:

- Provides a means for user authentication without the user needing to know the dashboard URL.
- Enables the provider to implement a captive portal, own the user experience, advertise value-added services, and build a brand experience.

Restrictions

SSG TCP Redirect for Services has the following restrictions:

- SSG TCP Redirect for Services requires Cisco SESM Release 3.1(1) to handle unauthenticated redirections. For other types of redirection, SESM Release 3.1.1 is required.

- The server defined in a server group must be globally routable.
- Traffic from hosts with overlapping IP addresses can be redirected only to SESMs with port bundle host keys.
- When overlapping IP address support is enabled (the host key feature is enabled), a host can reach the SSG only by a particular interface on the SSG. All packets between the host and the SSG use this interface and you should not change the route between the SSG and the host.
- Once the servers in a group have been configured, the routes to those servers should not change. SSG TCP Redirect for Services does not work if packets from servers that need to be redirected are received on a non-SSG interface.
- SSG TCP Redirect for Services does not support TCP sessions that can remain idle for more than one minute.

Related Features and Technologies

- Cisco Subscriber Edge Services Manager
- HTTP Redirect-Login in Cisco IOS Release 12.1(5)DC on 6400 series routers. See the “Service Selection Gateway” chapter of the *Cisco 6400 Feature Guide* for releases 12.1(5)DB and 12.1(5)DC for more information.
- Dynamic Subscriber Bandwidth Selection
- Hierarchical Policing in SSG
- PPPoA/PPPoE Autosense for ATM PVCs
- SSG Accounting Update Interval Per Service
- SSG AutoDomain
- SSG AutoLogoff and MAC Address in Accounting Records
- SSG AutoLogon Using Proxy Radius
- SSG Port–Bundle Host Key
- SSG Open Garden
- SSG Prepaid

Related Documents

- [APN Manager Application Programming Guide](#)
- [Cisco 6400 Software Configuration Guide and Command Reference](#)
- [Cisco Subscriber Edge Services Manager Documentation](#)
- [Cisco IOS Voice, Video, and Fax Command Reference](#), Release 12.2
- [Cisco IOS Voice, Video, and Fax Configuration Guide](#), Release 12.2
- [Configuring RADIUS](#)
- [Service Selection Gateway](#)
- [SSG AutoDomain](#)
- [SSG Autologoff](#)

- *SSG Autologin Using Proxy Radius*
- *Service Selection Gateway Hierarchical Policing*
- *SSG Open Garden*
- *SSG Port-Bundle Host Key*
- *SSG Prepaid*

Supported Platforms

- Cisco 6400 series
- Cisco 7200 series
- Cisco 7401ASR router

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- In order to use SSG TCP Redirect for Services, you must install Cisco SESM Release 3.1(1) to handle unauthenticated redirections. For other types of redirection, SESM Release 3.1.1 is required. (SMTP redirection is implemented completely within SSG and does not require a captive portal application.)

- You must enable Cisco Express Forwarding (CEF) on the router before SSG functionality can be enabled. If CEF is not enabled and you attempt to configure SSG, the following error message is displayed:

```
SSG: Please enable ip cef first
```



Note You can disable CEF at the individual interface level without affecting SSG.

Configuration Tasks

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional.



Note

SSG must be enabled by configuring the **ssg enable** command before these configurations can be completed. See the [Service Selection Gateway](#) feature module for Cisco IOS Release 12.2(4)B for detailed information about configuring SSG.

- [Enabling SSG TCP Redirect for Services](#) (required)
- [Defining a Captive Portal Group](#) (required)
- [Configuring the Redirection Group for Unauthenticated Users](#) (required)
- [Configuring TCP Ports for a Portal Group](#) (required)
- [Configuring Default Portal Groups for Captivation](#) (required)
- [Configuring Destination Networks](#) (required)
- [Configuring a Portal Group for SMTP Redirect](#) (optional)
- [Configuring the RADIUS Attributes for SSG TCP Redirect for Services](#) (optional)

Enabling SSG TCP Redirect for Services

To enable the SSG TCP Redirect for Services feature, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip cef	Enables CEF.
Step 2	Router(config)# ssg enable	Enables SSG functionality.
Step 3	Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.

Defining a Captive Portal Group

To configure a group of one or more servers that make up the captive portal group, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 2	Router(config-ssg-redirect)# server-group <i>group-name</i>	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode. <ul style="list-style-type: none"> <i>group-name</i>—Name of the captive portal group.
Step 3	Router(config-ssg-redirect-group)# server <i>ip-address</i> <i>port</i>	Adds a server to a captive portal group. <ul style="list-style-type: none"> <i>ip-address</i>—IP address of the server to add to the captive portal group. <i>port</i>—TCP port of the server to add to the captive portal group.

Configuring the Redirection Group for Unauthenticated Users

To select a captive portal group for redirection of traffic from unauthorized users, use the following commands beginning in global configuration mode command:

	Command	Purpose
Step 1	Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 2	Router(config-ssg-redirect)# redirect unauthenticated-user to <i>group-name</i>	Selects a captive portal group for redirection of traffic from unauthenticated users. <ul style="list-style-type: none"> <i>group-name</i>—Name of the captive portal group.

Configuring TCP Ports for a Portal Group

To define a port list, add TCP ports to a port list, and set a port or list of ports to be redirected by the captive portal group, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 2	Router(config-ssg-redirect)# port-list <i>port-listname</i>	Defines the port list and enters SSG-redirect-port configuration mode. <ul style="list-style-type: none"> <i>port-listname</i>—Defines the name of the port list.
Step 3	Router(config-ssg-redirect-port)# port <i>port-number</i>	Adds a port to a port list. <ul style="list-style-type: none"> <i>port-number</i>—Incoming destination port number. The valid range of port numbers is 1 to 65535

	Command	Purpose
Step 4	Router(config-ssg-redirect-port)# exit	Exits SSG-redirect-port configuration mode.
Step 5	Router(config-ssg-redirect)# redirect port <i>port-number to group-name</i> or Router(config-ssg-redirect)# redirect port-list <i>port-listname to group-name</i>	Configures a TCP port or named TCP port list for SSG TCP redirection. <ul style="list-style-type: none"> • port—Specifies a TCP port to mark for SSG TCP redirection. • port-list—Specifies the named TCP port list to mark for SSG TCP redirection. • <i>port-number</i>—Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection. • <i>group-name</i>—Defines the name of the captive portal group to redirect packets that are marked for a destination port or named TCP port list. • <i>port-listname</i>—Specifies the name of the named TCP port list.

Configuring Default Portal Groups for Captivation

To select the default captive portal group for initial captivation of users upon initialization (Account Logon), use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 2	Router(config-ssg-redirect)# redirect captivate initial default group <i>group-name duration seconds</i>	Selects the default captive portal group for initial captivation of users upon initialization. <ul style="list-style-type: none"> • <i>group-name</i>—Name of the captive portal group. • <i>seconds</i>—The duration in seconds of the initial captivation. The valid range is 1 to 65,536 seconds.
Step 3	Router(config-ssg-redirect)# redirect captivate advertising default group <i>group-name duration</i> <i>seconds frequency frequency</i>	Selects the default captive portal group for captivation of advertisements for users. <ul style="list-style-type: none"> • <i>group-name</i>—Name of the captive portal group. • <i>seconds</i>—The duration in seconds of the advertising captivation. The valid range is 1 to 65,536 seconds. • <i>frequency</i>—The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is 1 to 65,536 seconds.

Configuring Destination Networks

To configure a destination network for unauthorized service redirection, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 2	Router(config-ssg-redirect)# network-list <i>network-listname</i>	Defines the network list and enters SSG-redirect-network configuration mode. <ul style="list-style-type: none"> <i>network-listname</i>—Defines the name of the network list.
Step 3	Router(config-ssg-redirect-network)# network <i>ip-address</i>	Adds the specified IP address to the named network list. <ul style="list-style-type: none"> <i>ip-address</i>—The IP address to add to a named network list.
Step 4	Router(config-ssg-redirect-network)# exit	Exits SSG-redirect-network configuration mode.
Step 5	Router(config-ssg-redirect)# redirect unauthorized-service [destination network-list <i>network-listname</i>] to <i>group-name</i>	Creates a list of destination IP networks that can be redirected by the named captive portal group. <ul style="list-style-type: none"> (Optional) destination network-list—Checks incoming packets from authenticated hosts to networks that they are not authorized to access to determine if they need redirection. (Optional) <i>network-listname</i>—Name of the list of destination IP networks. <i>group-name</i>—Name of the captive portal group. <p>Note If you do not specify a destination IP network by configuring the optional destination network-list keywords, the captive portal group specified in the <i>group-name</i> attribute 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 the captive portal group.</p>

Configuring a Portal Group for SMTP Redirect

To select a captive portal group for redirection of Simple Mail Transfer Protocol (SMTP) traffic, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 2	Router(config-ssg-redirect)# redirect smtp group <i>group-name</i> [all user]	<p>Selects a captive portal group for redirection of SMTP traffic.</p> <ul style="list-style-type: none"> <i>group-name</i>—Name of the captive portal group. (Optional) all—All SMTP packets are forwarded. (Optional) user—SMTP packets from users that have SMTP forwarding permission are forwarded. <p>Note If you do not configure the optional all or user keywords, the default is all.</p>

Configuring the RADIUS Attributes for SSG TCP Redirect for Services

Configure the RADIUS attributes listed in this section in the user profiles on the AAA server. The user profile is downloaded from the AAA server as part of user authentication.

[Table 1](#) lists vendor-specific attributes needed in the user profile to perform SSG TCP redirection.

Table 1 Vendor-Specific RADIUS Attribute for the SSG TCP Redirect for Services Feature

Attribute ID	VendorID	SubAttrID	SubAttr Name	SubAttrDataType	Account-Info Feature Code
26	9	250	Account-Info	String	R

Allowable additional features:

- “S”—User has SMTP forwarding capability.
- “I*group*;duration[;service]”—User has initial captivation capability. This attribute also indicates the duration of the captivation in seconds. If you specify the optional *service* field, initial captivation starts only when the user activates the named service.
- “A*group*;duration;frequency[;service]”—User has advertisement captivation capability. Specifies the captive portal group to use, the duration and approximate frequency of the captivation in seconds. If you add the optional *service* field, advertisement captivation starts only when the user activates the named service.

Verifying SSG TCP Redirect for Services

Step 1 Use the **show running-config** command to verify configuration of SSG TCP Redirect for Services:

```
Router# show running-config
.
.
.
ssg tcp-redirect
 network-list RedirectNw
  network 172.16.10.0 255.255.255.0
  network 172.20.0.0 255.255.0.0
!
port-list WebPorts
 port 80
 port 8080
!
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 80 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
!
server-group CaptivateServer
 server 10.64.131.20 8000
!
 redirect port-list WebPorts to CaptivateServer
!
server-group SMTPServer
 server 10.64.131.20 25
!
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
```

Step 2 Use the **show ssg tcp-redirect group** [*group-name*] command in privileged EXEC command to:

- List all configured captive portal groups.
- Indicate which group is used for redirected packets from unauthorized users.
- Display which captive portal groups are the default groups for captivation and unauthorized service redirection.

If you do not enter the optional *group-name* attribute, the **show ssg tcp-redirect group** command displays a list of all defined portal groups. If the *group-name* attribute is included, the command displays information about the specified group.

```
Router# show ssg tcp-redirect group

Current TCP redirect groups:
RedirectServer
CaptivateServer
SMTPServer
SSD
```

```

Unauthenticated user redirect group:RedirectServer
Default service redirect group:SSD
SMTP forwarding group:SMTPServer, for all users
Default initial captivation group:CaptivateServer,
for 10 seconds
Default advertising captivation group:CaptivateServer,
for 30 seconds approximately every 3600 seconds

```

```
Router# show ssg tcp-redirect group RedirectServer
```

```

TCP redirect group RedirectServer:
Showing all TCP servers (Address, Port):
 10.2.36.253, 8080, FastEthernet0/0
Networks to redirect to (network-list RedirectNw):
 172.16.10.0 /24
 172.20.0.0 /16
TCP port to redirect:
 80

```

**Note**

This command replaces the **show ssg http-redirect** command.

Step 3

To verify any direct mappings, use the **show tcp-redirect mappings** [*ip-address* [*interface*]] command and check for the TCP redirect statements in the output.

If you do not enter the optional *ip-address* attribute, the **show tcp-redirect mappings** command displays a list of IP addresses for all hosts with stored mappings. If the *ip-address* attribute is included, any mappings for the host with the specified IP address are displayed. Use the optional *interface* attribute in port-bundle host key mode to specify the interface on which the host is connected to the SSG. Use the output displayed by this command to distinguish hosts with overlapping IP addresses.

```
Router# show tcp-redirect mappings
```

```

Authenticated hosts:
TCP remapping Host:172.16.10.0 to servers (IP:Port)
 10.2.36.253:8080
 10.64.131.20:25
### Total authenticated hosts being redirected = 1

Unauthenticated hosts:

TCP remapping Host:111.0.0.2 to server:10.2.36.253 on port:80 80

```

```
Router# show tcp-redirect mappings 172.16.0.0
```

```

TCP remapping Host:172.16.10.0
TCP remapping to server:10.2.36.253 on port:8080
Connection Mappings (src port <-> dest IP,dest port,timestamp, flags):
 11092 <-> 10.0.0.1,80,730967636,0x1
TCP remapping to server:10.64.131.20 on port:25
Connection Mappings (src port <-> dest IP,dest port,timestamp, flags):
 11093 <-> 10.0.0.1,25,730967652,0x0

```

**Note**

This command replaces the **show http-redirect mappings** command.

- Step 4** Use the **show ssg host *ip-address*** command to display information about a subscriber and current connections of the subscriber. The following example displays information about a subscriber connected at IP address 172.16.0.0:

```
Router# show ssg host 172.16.0.0

----- HostObject Content -----
Activated:TRUE
Interface:
User Name:dev-user1
Host IP:172.16.0.0
Msg IP:0.0.0.0 (0)
Host DNS IP:0.0.0.0
Maximum Session Timeout:0 seconds
Host Idle Timeout:0 seconds
Class Attr:NONE
User policing disabled
User logged on since:*07:20:57.000 UTC Mon Dec 3 2001
User last activity at:*07:20:59.000 UTC Mon Dec 3 2001
SMTP Forwarding:NO
Initial TCP captivate:YES
    (default) to group CaptivateServer for 10 seconds
TCP Advertisement captivate:YES
    (default) to group CaptivateServer for 10 seconds, approximately every 20 seconds
Default Service:NONE
DNS Default Service:NONE
Active Services:inet1;
AutoService:NONE
Subscribed Services:proxynat1; tunnell1; proxy1; passthru1;
Subscribed Service Groups:NONE
```

Monitoring and Maintaining SSG TCP Redirect for Services

Use the following commands to monitor the SSG TCP Redirect for Services feature:

Command	Purpose
Router# show ssg host <i>ip-address</i>	Displays information about a subscriber and current connections of the subscriber.
Router# show ssg tcp-redirect group [<i>group-name</i>]	Lists all configured captive portal groups and indicates which group receives redirected packets from unauthorized users. If the <i>group-name</i> attribute is specified, this command displays detailed information about that captive portal group.

Command	Purpose
Router# show tcp-redirect mappings [<i>ip-address</i> [<i>interface</i>]]	Displays the redirect mappings currently stored in SSG. If the host <i>ip-address</i> is provided, this command displays detailed redirect mapping information for the specified host. The TCP redirect mappings are removed automatically after the TCP session terminates or is idle for more than 60 seconds.
Router# debug ssg tcp-redirect { packet error event }	Use this command to turn on debug information for the SSG TCP Redirect for Services feature. <ul style="list-style-type: none"> • packet—Displays redirection information and any changes made to a packet when it is due for redirection. • error—Displays any SSG TCP redirect errors. • event—Displays any major SSG TCP redirect events or state changes. <p>Note This command replaces the debug ssg http-redirect command.</p>

Troubleshooting Tips

To display all debug TCP redirect information, use the **debug ssg tcp-redirect** command.

Configuration Examples

This section provides the following configuration examples:

- [Enabling SSG TCP Redirect for Services Example](#)
- [Defining a Captive Portal Group Example](#)
- [Configuring the Redirection Group for Unauthenticated Users Example](#)
- [Configuring TCP Ports for a Portal Group Examples](#)
- [Configuring a Default Portal Group for Captivation Example](#)
- [Configuring Destination Networks Examples](#)
- [Configuring a Portal Group for SMTP Redirect Examples](#)
- [Configuring the RADIUS Attributes for SSG TCP Redirect for Services Examples](#)

Enabling SSG TCP Redirect for Services Example

The following example shows how to enable the SSG TCP Redirect for Services feature:

```
ssg enable
ssg tcp-redirect
```

Defining a Captive Portal Group Example

The following example shows how to configure a group of one or more servers that make up the captive portal group. In the following example, the server with IP address 172.16.0.0 and port 8080 and the server with IP address 172.32.10.0 and port 8081 are added to the captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
  server-group RedirectServer
  server 172.16.0.0 8080
  server 172.32.10.0 8081
```

Configuring the Redirection Group for Unauthenticated Users Example

The following example shows how to select a captive portal group for redirection of traffic from unauthorized users. In the following example, traffic from unauthorized users is redirected to the captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
  redirect unauthenticated-user to RedirectServer
```

Configuring TCP Ports for a Portal Group Examples

The following example shows how to define a port list named “WebPorts” and adds TCP ports 80 and 8080 to the port list. Port 8080 is configured to be redirected by the captive portal group named “Redirect Server”:

```
ssg enable
ssg tcp-redirect
  port-list WebPorts
  port 80
  port 8080
  exit
  redirect port 8080 to RedirectServer
```

The following example shows how to define a port list named “WebPorts” and adds TCP ports 80 and 8080 to the port list. The port list named “WebPorts” is configured to be redirected by the captive portal group named “Redirect Server”:

```
ssg enable
ssg tcp-redirect
  port-list WebPorts
  port 80
  port 8080
  exit
  redirect port-list WebPorts to RedirectServer
```

Configuring a Default Portal Group for Captivation Example

The following example shows how to select the default captive portal group for initial captivation of users upon initialization (Account Logon) and the default captive portal group for advertising for a user. In the following example, the captive portal group named “InitialCaptiveGroup” is selected as the default destination for packets from a user for the first 10 seconds that user is connected. The portal group named “AdvertisingCaptiveGroup” is used to forward packets from a user for 20 seconds at an attempted frequency of once every hour (3600 seconds):

```
ssg enable
ssg tcp-redirect
  redirect captivate initial default group InitialCaptiveGroup duration 10
  redirect captivate advertising default group AdvertisingCaptiveGroup duration 20
frequency 3600
```

Configuring Destination Networks Examples

The following examples show how to configure a destination network for unauthorized service redirection.

In the following example, a network list named “RedirectNw” is created and configured as the default group for unauthorized service redirection. The networks at IP address 172.16.10.0 255.255.255.0 and 172.20.0.0 255.255.255.0 are added to the network list named “RedirectNw.”

```
ssg enable
ssg tcp-redirect
  network-list RedirectNw
    network 172.16.10.0 255.255.255.0
    network 172.20.0.0 255.255.255.0
  exit
  redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

In the following example, because no destination network list is specified, the captive portal group named “RedirectServer” is used as the default group for unauthorized service redirection.

```
ssg enable
ssg tcp-redirect
  network-list RedirectNw
    network 172.16.10.0 255.255.255.0
    network 172.20.0.0 255.255.255.0
  exit
  redirect unauthorized-service to RedirectServer
```

Configuring a Portal Group for SMTP Redirect Examples

The following examples show how to select a captive portal group for redirection of Simple Mail Transfer Protocol (SMTP) traffic.

In the following example, the captive portal group named “SMTPServer” is used to forward SMTP packets from any authorized user with the SMTP forwarding attribute.

```
ssg enable
ssg tcp-redirect
  redirect smtp group SMTPServer user
```

In the following example the captive portal group named “SMTPServer” is used to forward any SMTP packets from authorized users.

```
ssg enable
ssg tcp-redirect
redirect smtp group SMTPServer all
```

Configuring the RADIUS Attributes for SSG TCP Redirect for Services Examples



Note

The RADIUS attributes shown in the examples below are configured in the user profiles on the AAA server. The user profile is downloaded from the AAA server as part of user authentication.

The following example shows how to configure the user profile for initial captivation on account logon to one of the servers in the captive portal group named “CaptiveGrpA” for 300 seconds:

```
ICaptiveGrpA;300
```

The following example shows how to configure the user profile for initial captivation upon service logon to the service “Games”:

```
ICaptiveGrpB;240;Games
```

The following example shows how to configure the user for captivation of advertisements while the host is logged on to SSG:

```
ACaptiveGrpA;300;3600
```

The following example shows how to configure the user for captivation of advertisements to one of the servers in the captive portal group called “CaptiveGrpB” for 240 seconds, starting from when the user starts using the “Games” service and to attempt the captivation approximately every 1800 seconds:

```
ACaptiveGrpB;240;1800;Games
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications. Additional SSG commands can be found in the *SSG Commands for the Cisco 6400 NRP* document.

- [debug ssg http-redirect](#)
- [debug ssg tcp-redirect](#)
- [network \(ssg-redirect\)](#)
- [network-list](#)
- [port \(ssg-redirect\)](#)
- [port-list](#)
- [redirect captive advertising default group](#)
- [redirect captive initial default group duration](#)
- [redirect port to](#)
- [redirect smtp group](#)

- **redirect unauthenticated-user to**
- **redirect unauthorized-service to**
- **server**
- **server-group**
- **show http-redirect mappings**
- **show ssg http-redirect group**
- **show ssg tcp-redirect group**
- **show tcp-redirect mappings**
- **ssg http-redirect group**
- **ssg http-redirect group server**
- **ssg http-redirect port group**
- **ssg http-redirect unauthorized-user group**
- **ssg tcp-redirect**

debug ssg http-redirect

Beginning in Cisco IOS Release 12.2(4)B, the **debug ssg http-redirect** command is no longer supported and has been replaced by the **debug ssg tcp-redirect** command.

debug ssg tcp-redirect

To turn on debug information for the SSG TCP Redirect for Services feature, use the **debug ssg tcp-redirect** command in privileged EXEC mode.

debug ssg tcp-redirect {packet | error | event}

no debug ssg tcp-redirect {packet | error | event}

Syntax Description		
	packet	Displays redirection information and any changes made to a packet when it is due for redirection.
	error	Displays any SSG TCP redirect errors.
	event	Displays any major SSG TCP redirect events or state changes.

Defaults This command has no default behavior.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)B	Support for this command was integrated in Cisco IOS Release 12.2(4)B.

Usage Guidelines Use this command to turn on debug information for the SSG TCP Redirect for Services feature. Use the **packet** keyword to display redirection information and any changes made to a packet when it is due for redirection. Use the **error** keyword to display any SSG TCP redirect errors. Use the **event** keyword to display any major SSG TCP redirect events or state changes.



Note This command replaces the **debug ssg http-redirect** command.

Examples The following example shows how to display redirection information and any changes made to a packet when it is due for redirection:

```
Router# debug ssg tcp-redirect packet
```

Direction of the packet “-Up” indicates upstream packets from an SSG user, while “-Down” indicates downstream packets sent to a user:

```
07:13:15:SSG-REDIR-PKT:-Up:unauthorised user at 111.0.0.2 redirected to 9.2.36.253,8080
```

```
07:13:15:SSG-REDIR-PKT:-Down:TCP-RST Rxd for user at 111.0.0.2, port 11114
```

```
07:13:15:SSG-REDIR-PKT:-Down:return remap for user at 111.0.0.2 redirected from 9.2.36.25
```

The following example shows how to display any SSG TCP redirect errors:

```
Router# debug ssg tcp-redirect error
```

```
07:15:20:SSG-REDIR-ERR:-Up:Packet from 172.0.0.2:11114 has different destination from
stored connection
```

The following example shows how to display any major SSG TCP redirect events or state changes:

```
Router# debug ssg tcp-redirect event
```

Upstream packets from users are redirected:

```
06:45:51:SSG-TCP-REDIR:-Up:created new remap entry for unauthorised user at 172.16.0.2
06:45:51:          Redirect server set to 10.2.36.253,8080
06:45:51:          Initial src/dest port mapping 11094<->23
06:45:51:SSG-REDIR-EVT: Freeing tcp-remap connections
06:46:21:SSG-REDIR-EVT:Host at 111.0.0.2, connection port 11094 timed out
06:46:21:SSG-REDIR-EVT: Unauthenticated user remapping for 172.16.0.2 removed
```

A host is being activated:

```
06:54:09:SSG-REDIR-EVT:- New Host at 172.16.0.2 set for default initial captivation
06:54:09:SSG-REDIR-EVT:- New Host at 172.16.0.2 set for default advertising captivation
```

Initial captivation begins:

```
06:59:32:SSG-REDIR-EVT:-Up:initial captivate got packet at start of connection (from
111.0.0.2)
06:59:32:SSG-REDIR-EVT:-Up:user at 111.0.0.2 starting initial captivation
06:59:32:SSG-REDIR-EVT:- Up:created new redirect connection and server for user at
111.0.0.2
06:59:32:          Redirect server set to 10.64.131.20,8000
06:59:32:          Initial src/dest port mapping 11109<->80
06:59:48:SSG-REDIR-EVT:-Up:initial captivate got packet at start of connection (from
111.0.0.2)
06:59:48:SSG-REDIR-EVT:-Up:initial captivate timed out for user at 172.16.0.2
06:59:48:SSG-REDIR-EVT:Removing server 10.64.131.20:8000 for host 172.16.0.2
```

Advertising captivation begins:

```
06:59:48:SSG-REDIR-EVT:Removing redirect map for host 172.16.0.2
06:59:48:SSG-REDIR-EVT:-Up:advert captivate got packet at start of connection (from
111.0.0.2)
06:59:48:SSG-REDIR-EVT:-Up:user at 111.0.0.2 starting advertisement captivation
06:59:48:SSG-REDIR-EVT:- Up:created new redirect connection and server for user at
111.0.0.2
06:59:48:          Redirect server set to 10.64.131.20,8000
06:59:48:          Initial src/dest port mapping 11110<->80
```

Related Commands

Command	Description
ssg enable	Enables SSG.
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 tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

network (ssg-redirect)

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*

no network *ip-address*

Syntax Description	<i>ip-address</i>	The IP address to add to a named network list.
Defaults	No default behavior or values.	
Command Modes	SSG-redirect-network	
Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines

Use this command to define an individual network that is found in a named network list. Use the **network-list** *network-listname* 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 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. 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:

```
network-list RedirectNw
network 10.0.0.0 255.0.0.0
network 10.2.2.0 255.255.255.0
```

■ network (ssg-redirect)

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

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

<i>network-listname</i>	Defines the name of the network list.
-------------------------	---------------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect

Command History

Release	Modification
12.2(4)B	This command was introduced.

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 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. 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.

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

port (ssg-redirect)

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 port** form of this command.

port *port-number*

no port *port-number*

Syntax Description	<i>port-number</i>	Incoming destination port number.
--------------------	--------------------	-----------------------------------

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	SSG-redirect-port
---------------	-------------------

Command History	Release	Modification
	12.2(4)B	This command was introduced.

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** command. Define and name the TCP port list using the **port-list** 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 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	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.

Command	Description
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

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

<i>port-listname</i>	Defines the name of the port list.
----------------------	------------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect

Command History

Release	Modification
12.2(4)B	This command was introduced.

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 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 port to	Marks a TCP port or named TCP port list for SSG TCP redirection.
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.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.

Command	Description
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
<code>ssg enable</code>	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect captive advertising default group

To configure the default captive portal group, duration, and frequency for advertising captivation, use the **redirect captive 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 captive advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

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

Syntax Description		
	<i>group-name</i>	Name of the captive portal group.
	<i>seconds</i>	The duration in seconds of the advertising captivation. The valid range is 1 to 65,536 seconds.
	<i>frequency</i>	The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is 1 to 65,536 seconds.

Defaults No default behavior or values.

Command Modes SSG-redirect

Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines Use this command to select the default captive portal group for advertising captivation of users upon Account Logon. Use the *seconds* attribute 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* attribute.

Use the *frequency* attribute to configure how often 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 “AdvertisingCaptiveServer” to forward packets from a user for 30 seconds at an interval of every 3600 seconds:

```
redirect captive advertising default group AdvertisingCaptiveServer duration 30
frequency 3600
```

Related Commands	Command	Description
	redirect captive initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
	redirect port 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 Simple Mail Transfer Protocol (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 captive initial default group duration

To select a default captive portal group and duration of the initial captivation of users on Account Logon, use the **redirect captive initial default group duration** 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 captive initial default group *group-name* **duration** *seconds*

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

Syntax Description		
	<i>group-name</i>	Name of the captive portal group.
	<i>seconds</i>	The duration in seconds of the initial captivation. The valid range is 1 to 65,536 seconds.

Defaults No default behavior or values.

Command Modes SSG-redirect

Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines Use this command to select the default captive portal group for initial captivation of users on Account Logon. Use the *seconds* attribute 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* attribute.

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 “InitialCaptiveServer” will be used to forward packets from a user for the first 10 seconds that the user is connected:

```
redirect captive initial default group InitialCaptiveServer duration 10
```

Related Commands	Command	Description
	redirect captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
	redirect port 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 Simple Mail Transfer Protocol (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 port to

To configure a TCP port or named TCP port list for SSG TCP Redirect for Services, use the **redirect port 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.
<i>port-listname</i>	Specifies the name of the named TCP port list.
port	Specifies a TCP port to mark for SSG TCP redirection.
<i>port-number</i>	Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
<i>group-name</i>	Defines the name of the captive portal group to redirect packets that are marked for a destination port or named TCP port list.

Defaults

No default behavior or values.

Command Modes

SSG-redirect

Command History

Release	Modification
12.2(4)B	This command was introduced.

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”:

```
redirect port 8080 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”:

```
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 duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect unauthorized-service to server	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
server-group	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 smtp group

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	
<i>group-name</i>	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.

Defaults The keyword **all** is the default if no keyword is specified.

Command Modes SSG-redirect

Command History	Release	Modification
	12.2(4)B	This command was introduced.

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* attribute. 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 show how to configure all SMTP packets from authorized users to be redirected to the captive portal group named “SMTPServer”:

```
redirect smtp group SMTPServer all
```

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 duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
	redirect port 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 unauthenticated-user to

To redirect TCP traffic from unauthenticated users to a specified captive portal group, use the **redirect unauthenticated-user to** command in 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

<i>group-name</i>	The name of the captive portal group.
-------------------	---------------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect

Command History

Release	Modification
12.2(4)B	This command was introduced.

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":

```
redirect unauthenticated-user to RedirectServer
```

Related Commands

Command	Description
redirect captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect port 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 Simple Mail Transfer Protocol (SMTP) traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.

Command	Description
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 to

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

Defaults No default behavior or values.

Command Modes SSG-redirect

Command History	Release	Modification
	12.2(4)B	This command was introduced.

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* attribute. 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* attribute 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 to 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 to 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 a packet’s destination matches one of the networks in the destination IP network list named “RedirectNW”:

```
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 a packet’s destination 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 duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect port 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 Simple Mail Transfer Protocol (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.

server

To add a server to a captive portal group, use the **server** command in SSG-redirect-group configuration mode. To remove a server from a captive portal group, use the **no** form of this command.

server *ip-address port*

no server *ip-address port*

Syntax Description	<i>ip-address</i>	IP address of the server to add to the captive portal group.
	<i>port</i>	TCP port of the server to add to the captive portal group.

Defaults No default behavior or values.

Command Modes SSG-redirect-group

Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines Use the **server** command in SSG-redirect-group configuration mode to add a server, defined by its IP address and TCP port, to a captive portal group.

SSG TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

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 captive portal group. Use the **server-group** command in SSG-redirect configuration mode to create and name a captive portal group before using the **server** command to add servers to the captive portal group.

Examples The following example adds a server at IP address 10.0.0.0 and TCP port 8080 and a server at IP address 10.1.2.3 and TCP port 8081 to a captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
server-group RedirectServer
server 10.0.0.0 8080
server 10.1.2.3 8081
```

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-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.

server-group

To define the group of one or more servers that make up a named captive portal group and enter SSG-redirect-group configuration mode, use the **server-group** command in SSG-redirect configuration mode. To remove a captive portal group and any servers configured within that portal group, use the **no** form of this command.

server-group *group-name*

no server-group *group-name*

Syntax Description	<i>group-name</i>	The name of the captive portal group.
---------------------------	-------------------	---------------------------------------

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	SSG-redirect
----------------------	--------------

Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines Use this command to define and name a captive portal group. SSG TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

After defining a captive portal group with the **server-group** command, identify individual servers for inclusion in the captive portal group using the **server** *ip-address port* command in SSG-redirect-group configuration mode.

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 captive portal group.



Note

This command, along with the **server** command, replaces the **ssg http-redirect group** *group-name* **server** *ip-address port* command.

Examples The following example defines a captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
server-group RedirectServer
```

Related Commands	Command	Description
	server	Adds a server to a 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.

show http-redirect mappings

Beginning in Cisco IOS Release 12.2(4)B, the **show http-redirect mappings** command is no longer supported and has been replaced by the [show tcp-redirect mappings](#) command.

show ssg http-redirect group

Beginning in Cisco IOS Release 12.2(4)B, the **show ssg http-redirect group** command is no longer supported and has been replaced by the **show ssg tcp-redirect group** command.

show ssg tcp-redirect group

To display information about the captive portal groups and their networks associated with those portal groups, use the **show ssg tcp-redirect group** privileged EXEC command.

```
show ssg tcp-redirect group [group-name]
```

Syntax Description	<i>group-name</i> (Optional) The previously-defined name for the captive portal group.
---------------------------	--

Defaults	No default behaviors or values.
-----------------	---------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines Use this command to display information about the captive portal groups and their associated networks defined in your system.

If you omit the optional *group-name* field, this command displays a list of all defined captive portal groups and the networks associated with the captive portal groups. If you specify the *group-name* attribute, this command displays information about that group and its associated networks.



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

Examples The example below shows how to display a list of all of the defined captive portal groups:

```
Router# show ssg tcp-redirect group

Current TCP redirect groups:
RedirectServer
CaptivateServer
SMTPServer
SSD

Unauthenticated user redirect group:RedirectServer
Default service redirect group:SSD
SMTP forwarding group:SMTPServer, for all users
Default initial captivation group:CaptivateServer,
for 10 seconds
Default advertising captivation group:CaptivateServer,
for 30 seconds approximately every 3600 seconds
```

```
show ssg tcp-redirect group
```

Table 2 describes the significant fields shown in the display above.

Table 2 *show ssg tcp-redirect group Field Descriptions*

Field	Description
Current TCP redirect groups:	List of all TCP-redirect groups.
Default service redirect group: SSD	Default service redirect group.
SMTP forwarding group: SMTPServer, for all users	SMTP redirection settings.
Default initial captivation group: CaptivateServer, for 10 seconds	Default initial captivation group, name of captivation, and duration of captivation.
Default advertising captivation group: CaptivateServer, for 30 seconds approximately every 3600 seconds	Default advertising captivation group, name of captivation group, duration, and frequency of advertising captivation.

The example below shows how to display a detailed description of the captive portal group called “RedirectServer”:

```
Router# show ssg tcp-redirect group RedirectServer

TCP redirect group RedirectServer:
Showing all TCP servers (Address, Port):
 10.2.36.253, 8080, FastEthernet0/0
Networks to redirect to (network-list RedirectNw):
 172.16.10.0 /24
 172.20.0.0 /16
TCP port to redirect:
 80
```

Table 3 describes the significant fields shown in the display above.

Table 3 *show ssg tcp-redirect group group-name Field Descriptions*

Field	Description
Showing all TCP servers (Address, Port):	List of all servers.
10.2.36.253	Server IP address.
8080	Server port number.
FastEthernet0/0	Interface on which this server is reachable.
Networks to redirect to	List of networks.
(network-list RedirectNw):	Network list name.
TCP port to redirect:	Name of port-list (if port-list is used).

Related Commands

Command	Description
debug ssg tcp-redirect	Turns on debug information for the SSG TCP Redirect for Services feature.
network (ssg-redirect)	Adds an IP address to a named network list.
network-list	Defines a list of one or more IP networks that make up a named network list.

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 captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect port 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 Simple Mail Transfer Protocol (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 authenticated users to a specified captive portal group.
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.
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.

show tcp-redirect mappings

To display information about the TCP redirect mappings for hosts within your system, use the **show tcp-redirect mappings** command in privileged EXEC mode.

show tcp-redirect mappings [*ip-address* [*interface*]]

Syntax Description		
	<i>ip-address</i>	(Optional) Displays redirection mappings for this specific host.
	<i>interface</i>	(Optional) Displays redirection mappings for the host connected to SSG on the specified downlink interface.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines Use this command to display information about the TCP redirect mappings for hosts within your system. If you omit the optional *ip-address* attribute, this command displays a list of all host IP addresses that currently have stored mappings. If you include the *ip-address* attribute, this command displays any mappings for the host with the specified IP address. You can use the *interface* attribute when SSG is running in port mapped host key mode to specify the downlink interface on which the host is connected to the SSG. Use the *interface* attribute when you want to display information about a specific host where there are overlapping IP addresses among hosts.

The TCP redirect mappings are removed automatically after the TCP session terminates or is idle for more than 60 seconds.



Note

This command replaces the **show http-redirect mappings** command.

Examples The following example displays all of the hosts that have redirect mappings stored on your system:

```
Router# show tcp-redirect mappings

Authenticated hosts:
  TCP remapping Host:172.16.10.0 to servers (IP:Port)
    10.2.36.253:8080
    10.64.131.20:25
### Total authenticated hosts being redirected = 1

Unauthenticated hosts:

TCP remapping Host:172.0.0.2_to server:10.2.36.253 on port:8080
```

The following example displays detailed mapping for the host at IP address 172.16.0.0:

```
Router# show tcp-redirect mappings 172.16.0.0

TCP remapping Host:172.16.0.0
TCP remapping to server:10.2.36.253 on port:8080
Connection Mappings (src port <-> dest IP,dest port,timestamp, flags):
    11092 <-> 10.0.0.1,80,730967636,0x1
TCP remapping to server:10.64.131.20 on port:25
Connection Mappings (src port <-> dest IP,dest port,timestamp, flags):
    11093 <-> 10.0.0.1,25,730967652,0x0
```

Table 4 describes the significant fields shown in the displays above.

Table 4 *show tcp-redirect mappings Field Descriptions*

Field	Description
Authenticated hosts	List of all authenticated hosts having mappings.
TCP remapping Host:172.16.10.0	Host IP address.
10.2.36.253:8080	List of server and port to which this host is being redirected.
Unauthenticated hosts	List of unauthenticated host IP addresses.
TCP remapping Host:172.0.0.2	Unauthenticated host IP address.
to server:10.2.36.253 on port:8080	Server IP address and port.
dest IP,dest port,timestamp	Timestamp when the last packet was translated using this mapping.
0x1	State of the TCP connection. 0x0 indicates a fully active session. Other values can indicate that the session has shut down partially or fully. 0x01 indicates a session reset. 0x1E indicates the session has terminated.

Related Commands

Command	Description
debug ssg tcp-redirect	Turns on debug information for the SSG TCP Redirect for Services feature.
network (ssg-redirect)	Adds an IP address to a named network list.
network-list	Defines a list of one or more IP networks that make up a named network list.
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 captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect port to	Marks a TCP port or named TCP port list for SSG TCP redirection.

Command	Description
redirect smtp group	Selects a captive portal group for redirection of Simple Mail Transfer Protocol (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 authenticated users to a specified captive portal group.
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.
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.

ssg http-redirect group

Beginning in Cisco IOS Release 12.2(4)B, the **ssg http-redirect group** command is no longer supported and has been replaced by the **ssg tcp-redirect** command.

ssg http-redirect group server

Beginning in Cisco IOS Release 12.2(4)B, the **ssg http-redirect group** *group-name* **server** *ip-address port* command is no longer supported and has been replaced by the **server** and **server-group** commands.

ssg http-redirect port group

Beginning in Cisco IOS Release 12.2(4)B, the **ssg http-redirect port group** command is no longer supported and has been replaced by the **redirect port to** command.

ssg http-redirect unauthorized-user group

Beginning in Cisco IOS Release 12.2(4)B, the **ssg http-redirect unauthorized-user group** command is no longer supported and has been replaced by the **redirect unauthenticated-user to** command.

ssg tcp-redirect

To enable SSG TCP redirection and enter SSG-redirect mode, use the **ssg tcp-redirect** command. To disable SSG TCP redirection, use the **no** form of this command.

ssg tcp-redirect

no ssg tcp-redirect

Syntax Description This command has no arguments or keywords.

Defaults This command has no default behavior.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)B	This command was introduced.

Usage Guidelines Use this command to enable SSG TCP redirection. This command also enables SSG-redirect mode. The **no ssg tcp-redirect** command disables SSG TCP redirection and removes all configurations created in the SSG-redirect mode. You must enable SSG by issuing the **ssg enable** command before you can configure SSG TCP redirection.



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

Examples The following example enables SSG and SSG TCP redirection:

```
ssg enable
ssg tcp-redirect
```

Related Commands	Command	Description
	debug ssg tcp-redirect	Turns on debug information for the SSG TCP Redirect for Services feature.
	network (ssg-redirect)	Adds an IP address to a named network list.
	network-list	Defines a list of one or more IP networks that make up a named network list.
	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.

Command	Description
redirect captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect port 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 Simple Mail Transfer Protocol (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 server	Redirects TCP traffic from authenticated users to a specified captive portal group.
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.
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.

Replaced Commands

Beginning in Cisco IOS Release 12.2(4)B, some SSG commands have been replaced by other commands. [Table 5](#) maps the old commands to their replacements.

Table 5 Replaced Commands

Old Command	New Command
debug ssg http-redirect	debug ssg tcp-redirect
show http-redirect mappings	show tcp-redirect mappings
show ssg http-redirect group	show ssg tcp-redirect group
ssg http-redirect group	ssg tcp-redirect
ssg http-redirect group server	server-group and server
ssg http-redirect port group	redirect port to
ssg http-redirect unauthorized-user group	redirect unauthenticated-user to

Glossary

captive portal—Captive portals enable service providers to capture a subscriber's attention with targeted messages such as authentication, advertising, requests for per-service payment, and blocked access to a particular service.

host key—Combination of port bundle and SSG source IP address that uniquely identifies a subscriber.

open garden—Collection of websites or networks that users can access without having to provide authentication information.

packet—The unit of data sent across a packet-switching network.

port—The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

RADIUS—Remote Authentication Dial-In User Service. A client/server security protocol created by Livingston Enterprises. Security information is stored in a central location, known as the RADIUS server.

SESM—Subscriber Edge Services Manager. Successor product to the Cisco SSD. SESM is part of a Cisco solution that allows subscribers of DSL, cable, wireless, and dial-up to simultaneously access multiple services provided by different Internet service providers, application service providers, and Corporate Access Servers.

SSD—Service Selection Dashboard. A customizable Web-based application that works with the Cisco SSG to allow end customers to log on to and disconnect from proxy and passthrough services through a standard Web browser. After the customer logs in to the service provider's network, an HTML Dashboard is populated with the services authorized for that user.

SSG—Service Selection Gateway. The Cisco SSG offers service providers a means for menu-based service selection. End users can select services from the Dashboard menu, and the Cisco SSG sets up and tears down proxy and passthrough network connections based on a user's selection. The Cisco SSG accounts for the services selected so that service providers can bill for individual services.

TCP—Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

VSA—Vendor-Specific Attribute. An attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair.

