



SSG Permanent TCP Redirection

The SSG Permanent TCP Redirection feature enables Service Selection Gateway (SSG), in conjunction with Cisco Subscriber Edge Services Manager (SESM), to provide service selection support to users whose web browsers are configured with HTTP proxy servers. This feature supports plug-and-play functionality in public wireless LANs.

Feature History for the SSG Permanent TCP Redirection Feature

Release	Modification
12.3(3)B	This feature was introduced.
12.3(7)T	This feature was integrated into Cisco IOS Release 12.3(7)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for SSG Permanent TCP Redirection, page 2](#)
- [Restrictions for SSG Permanent TCP Redirection, page 2](#)
- [Information About SSG Permanent TCP Redirection, page 2](#)
- [How to Configure SSG Permanent TCP Redirection, page 5](#)
- [Configuration Examples for SSG Permanent TCP Redirection, page 9](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)
- [Glossary, page 17](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Prerequisites for SSG Permanent TCP Redirection

Before permanent TCP redirection can be configured, SSG must be enabled by using the **ssg enable** command.

The SSG TCP Redirect feature must be enabled by using the **ssg tcp-redirect** command.

See the [Glossary](#) for definitions of terms used in this document.

Restrictions for SSG Permanent TCP Redirection

The SSG Permanent TCP Redirection feature has the following restrictions:

- SSG will not provide concurrent service selection to the HTTP proxy user who uses web traffic to reach more than one service. SSG can redirect web traffic to only one service or server.



Note You can use the Cisco Content Service Gateway (CSG) as the HTTP proxy server in the SSG configurations. SSG will then send all the HTTP traffic to CSG, which can provide service selection to these users.

- SSG will not provide TCP redirection for unauthorized services for HTTP proxy users who are unauthenticated because SSG will not know the destination of the traffic.



Note You can use CSG as the authenticated HTTP server in the SSG configurations. SSG will send the HTTP traffic to CSG, which can recognize an unauthorized access attempt by a user and take appropriate action.

- SSG simulates the proxy for HTTP traffic, so if a user tries to send any traffic other than HTTP traffic, the connection will fail. For example, a user will be unable to use FTP to access the HTTP proxy server configured in the browser.
- If a user changes HTTP proxy settings after authentication, SSG will not be able to detect the changes.

Information About SSG Permanent TCP Redirection

To configure SSG permanent TCP redirection for HTTP proxy support, you should understand the following concepts:

- [Overview of SSG, page 3](#)
- [How SSG Permanent TCP Redirection Works, page 3](#)
- [Supported SSG Permanent TCP Redirection Functionality, page 4](#)
- [RADIUS Attributes for SSG Permanent TCP Redirection, page 5](#)
- [Benefits of SSG Permanent TCP Redirection, page 5](#)

2. The user tries to open a web page; for example, `http://www.example.com`. The browser sends the traffic to the HTTP proxy server (`IPw : Portw`).
3. SSG intercepts the traffic from unauthenticated user `IPu` and passes it to the SESM captive portal.
4. The SESM captive portal looks into the HTTP packet and determines if the packet is destined for the HTTP proxy server. When the SESM captive portal determines that the packet is destined for an HTTP proxy server, it sends a message to SSG containing the user's HTTP proxy settings.
5. SSG stores the information (namely, that user `IPu` has the HTTP proxy server setting `IPw : Portw`). From now on, SSG will redirect all traffic from user `IPu` and destined for `IPw : Portw` to the local HTTP proxy server for unauthenticated users, which is running on SESM.
6. Once the user has been authenticated, SSG will redirect all traffic from the user `IPu` and destined for `IPw : Portw` to the local HTTP proxy server for authenticated users, which is also running on SESM.

Supported SSG Permanent TCP Redirection Functionality

The SSG Permanent TCP Redirection feature supports the following functionality:

- SSG will allow users whose browsers are configured with HTTP proxy servers to log on and reach the Internet. The HTTP proxy server can be configured as an IP address or a domain name.
- SSG supports users with HTTP proxy server configurations who also use Extensible Authentication Protocol (EAP) authentication methods by redirecting the users to the SESM captive portal using the initial-captivation functionality.
- SSG supports users with HTTP proxy server configurations in PWLAN hot spots in which the hot spot allows users to select from multiple ISPs. In such cases, each ISP must have an instance of the HTTP proxy server running on SESM, and this instance can be defined in the ISP's service profile. ISPs can share the same HTTP server.
- SSG will allow the user to initiate an end-to-end Virtual Private Network (VPN) connection after the user has been authenticated and authorized to reach the Internet or VPN gateway.
- If an authenticated user selects a corporate service (a Layer 2 Tunnel Protocol (L2TP) tunnel service that is initiated from SSG), the service can be configured so that SSG allows HTTP traffic to reach the service without redirecting it to the local HTTP proxy server.



Note The corporate HTTP proxy server must be able to reach SESM in order for users to be able to log out or manage services. To enable HTTP proxy users to reach SESM, give SESM a globally routable IP address.

- SSG permanent TCP redirection is supported with or without the SSG Port-Bundle Host Key feature.
- SSG will include in its accounting all the HTTP traffic going to the HTTP proxy server, even traffic destined for the open garden or TCP-redirect server (which is otherwise not included in the accounting).

**Note**

If you use the CSG as the authenticated HTTP server, you can configure the CSG to prevent HTTP traffic destined for the open garden or TCP redirect server from being included in accounting.

- The SSG Permanent TCP Redirection feature is supported even if the user is configured with an exclude list for the HTTP proxy server and the home page (or first page) falls into the exclude list.

RADIUS Attributes for SSG Permanent TCP Redirection

Table 1 lists the vendor-specific attributes that can be configured in the RADIUS service profile to perform SSG permanent TCP redirection. The service profile is downloaded from the authentication, authorization, and accounting (AAA) server as part of user authentication.

Table 1 Vendor-Specific RADIUS Attributes for the SSG Permanent TCP Redirection Feature

Attribute ID	Vendor ID	Subattribute ID	Subattribute Type	Subattribute Data
26	9	251	Service-Info	<p><i>KWserver-group-name</i>—When a user logs in to the service, SSG redirects the user’s HTTP traffic to a server in the specified server group. All the service features (such as quality of service (QoS) and prepaid billing) are applied to the HTTP traffic.</p> <p>Example: <code>ssg-service-info = KWhttp-proxy-isp_a</code></p>
26	9	251	Service-Info	<p><i>KW0</i>—When a user logs in to the service, SSG allows all HTTP traffic to go to the service without redirection as if there were no HTTP-proxy server settings in the user’s browser.</p> <p>The service network entries must include the actual HTTP proxy address.</p> <p>This subattribute takes precedence over the 26,9,251 <i>KWserver-group-name</i> attribute.</p> <p>Example: <code>ssg-service-info = KW0</code></p>

Benefits of SSG Permanent TCP Redirection

The SSG Permanent TCP Redirection feature enables SSG to provide service selection support to users whose web browsers are configured with HTTP proxy servers. This solution enables SSG, in conjunction with SESM, to provide an emulation of the HTTP proxy so the experience of the user is as if the user’s web browser were exchanging traffic with the user’s real HTTP proxy server. This feature supports plug-and-play functionality in PWLANs.

How to Configure SSG Permanent TCP Redirection

This section contains the following procedures:

- [Defining a Captive Portal Group, page 6](#)

- [Configuring SSG Permanent TCP Redirection for HTTP Proxy Support, page 7](#)
- [Verifying SSG Permanent TCP Redirection, page 8](#)

Defining a Captive Portal Group

Perform this task to configure captive portal server groups for authenticated and unauthenticated HTTP-proxy users.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **server-group** *group-name*
5. **server** *ip-address port*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ssg tcp-redirect Example: Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 4	server-group <i>group-name</i> Example: Router(config-ssg-redirect)# server-group unauth_http_group	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"> • You can configure a separate server group for authenticated and unauthenticated HTTP proxy users. • <i>group-name</i>—Name of the captive portal group.

	Command or Action	Purpose
Step 5	<pre>server ip-address port</pre> <p>Example: Router(config-ssg-redirect-group)# server 10.2.76.12 80 </p>	<p>Adds a server to a captive portal group.</p> <ul style="list-style-type: none"> <i>ip-address</i>—IP address of the server to be added to the captive portal group. <i>port</i>—TCP port of the server to be added to the captive portal group.
Step 6	<pre>end</pre> <p>Example: Router(config-ssg-redirect-group)# end </p>	(Optional) Returns to global configuration mode.

Configuring SSG Permanent TCP Redirection for HTTP Proxy Support

Perform this task to configure permanent TCP redirection for authenticated and unauthenticated users with HTTP proxy server configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **redirect permanent http authenticated to *server-group***
5. **redirect permanent http unauthenticated to *server-group***
6. **end**
7. Configure the RADIUS service profile to support permanent TCP redirection.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>ssg tcp-redirect</pre> <p>Example: Router(config)# ssg tcp-redirect </p>	Enables SSG TCP redirect and enters SSG-redirect configuration mode.

	Command or Action	Purpose
Step 4	<pre>redirect permanent http authenticated to server-group</pre> <p>Example: Router(config-ssg-redirect)#</p>	<p>Specifies a server group for permanent TCP redirections for authenticated users with HTTP proxy server configurations.</p> <ul style="list-style-type: none"> <i>server-group</i>—name of the local HTTP proxy server group for authenticated users
Step 5	<pre>redirect permanent http unauthenticated to server-group</pre> <p>Example: Router(config-ssg-redirect)#</p>	<p>Specifies a server group for permanent TCP redirections for unauthenticated users with HTTP proxy server configurations.</p> <ul style="list-style-type: none"> <i>server-group</i>—name of the local HTTP proxy server group for unauthenticated users
Step 6	<pre>end</pre> <p>Example: Router(config-ssg-redirect)# end</p>	<p>(Optional) Returns to global configuration mode.</p>
Step 7	<p>Configure the RADIUS service profile to support permanent TCP redirection.</p>	<p>The RADIUS service profile is downloaded from the AAA server as part of service authorization. Configure one of the following attributes in the service profile to support permanent TCP redirection:</p> <ul style="list-style-type: none"> ssg-service-info = KW<i>server-group-name</i> ssg-service-info = KW0 <p>See the “RADIUS Attributes for SSG Permanent TCP Redirection” section on page 5 for more information about the RADIUS attributes for permanent TCP redirection.</p>

Verifying SSG Permanent TCP Redirection

Perform this task to verify the configuration and functionality of SSG permanent TCP redirection for HTTP proxy support.

SUMMARY STEPS

1. **show ssg tcp-redirect mappings** [*ip-address* [*interface*]]
2. **show ssg host** [*ip-address* [*interface*] | *username*]
3. **show ssg connection** *ip-address service-name* [*interface*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>show ssg tcp-redirect mappings [ip-address [interface]]</pre> <p>Example: Router# show ssg tcp-redirect mappings</p>	<p>Displays information about the TCP redirect mappings for hosts within your system.</p> <ul style="list-style-type: none"> Use the show ssg tcp-redirect mappings command to display permanent TCP redirect mappings for unauthenticated and authenticated users.
Step 2	<pre>show ssg host [ip-address [interface] username]</pre> <p>Example: Router# show ssg host</p>	<p>Displays information about a user and the current HTTP proxy status of the user.</p> <ul style="list-style-type: none"> When HTTP traffic is redirected to the default HTTP proxy server for authenticated users, the input and output counters for bytes and packets are included in the accounting for the host. Use the show ssg host command to display these statistics.
Step 3	<pre>show ssg connection ip-address service-name [interface]</pre> <p>Example: Router# show ssg connection</p>	<p>Displays the connections of a given host and service name.</p> <ul style="list-style-type: none"> Use the show ssg connection command to display connection information for a specific host and service when the 26,9,251,KWserver-group-name attribute is configured in the service profile for the service.

Configuration Examples for SSG Permanent TCP Redirection

- [Configuring SSG for Permanent TCP Redirection: Example, page 9](#)
- [Configuring RADIUS Attributes for Permanent TCP Redirection: Example, page 10](#)
- [Verifying SSG Permanent TCP Redirection: Examples, page 10](#)

Configuring SSG for Permanent TCP Redirection: Example

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 10.76.86.90 8090
!
server-group auth_web_group
  server 10.76.86.90 8101
!
server-group unauth_web_group
  server 10.76.86.90 8102
!
redirect unauthenticated-user to unauthen-group
!
redirect permanent http unauthenticated to unauth_web_group
!
redirect permanent http authenticated to auth_web_group
```

Configuring RADIUS Attributes for Permanent TCP Redirection: Example

The RADIUS attributes shown in the examples below are configured in the service profiles on the AAA server.

The following example shows how to configure the service profile so that when a user logs on to the service, SSG will redirect the user's HTTP traffic to a server configured in the server group called "service_http_proxy_isp_a":

```
ssg-service-info = KWservice_http_proxy_isp_a
```

The following example shows how to configure the service profile so that when a user logs on to the service, SSG will allow all HTTP traffic to go to the service without permanent TCP redirection:

```
ssg-service-info = KW0
```

Verifying SSG Permanent TCP Redirection: Examples

The following examples show a basic configuration and corresponding sample output for the commands that can be used to verify the SSG Permanent TCP Redirection feature:

- [show ssg tcp-redirect mappings Sample Output: Example, page 10](#)
- [show ssg host Sample Output: Example, page 11](#)
- [show ssg connection Sample Output: Example, page 12](#)

show ssg tcp-redirect mappings Sample Output: Example

Use the **show ssg tcp-redirect mappings** command to display permanent TCP redirect mappings for unauthenticated users.

The examples that follow correspond to this configuration example:

```
!
ssg tcp-redirect
  server-group unauthen-group
    server 10.76.86.90 80
  !
  redirect unauthenticated-user to unauthen-group
  !
  server-group unauth_web_group
    server 9.2.76.12 80
  !
  redirect permanent http unauthenticated to unauth_web_group
```

The following output corresponds to the sample configuration above:

```
Router# show ssg tcp-redirect mappings

Authenticated hosts:
  No TCP redirect mappings for authenticated users

Unauthenticated hosts:
  TCP remapping Host:1.6.6.2 to server:10.76.86.90 on port:80
  Host:1.6.6.2 has web-proxy settings 160.0.0.2:3123

Total number of hosts with mappings: 1
```

```

Router# show ssg tcp-redirect mappings 1.6.6.2

TCP remapping Host:1.6.6.2 to server:10.76.86.90 on port:80
Connection Mappings (src port <-> dest IP,dest
port,timestamp,flags,upst_seq,upst_ack,dnst_seq,dnst_ack):
    24706 <-> 160.0.0.2,3123,1062436827,0x0,102D9680,C0368148,C0368148,102D9680
TCP remapping Host:1.6.6.2 to server: 9.2.76.12 on port:80 (1:0)
Connection Mappings (src port <-> dest IP,dest
port,timestamp,flags,upst_seq,upst_ack,dnst_seq,dnst_ack):
    30850 <-> 150.0.0.2,23,1068514862,0x0,4092DF40,EC073184,EC07317E,4092DF40

User has permanent web-redirect settings: 160.0.0.2:3123 is redirected to 9.2.76.12:80,
last-activity at:1062436830

```

show ssg host Sample Output: Example

When HTTP traffic is redirected to the default HTTP proxy server for authenticated users, the input and output counters for bytes and packets are included in the accounting for the host. Use the **show ssg host** command to display these statistics.

The examples that follow correspond to this configuration example:

```

!
ssg tcp-redirect
  server-group auth_web_group
  server 9.2.36.253 80
!
redirect permanent http authenticated to auth_web_group

```

The following output corresponds to the sample configuration above:

```

Router# show ssg host 1.6.6.2

User has permanent web-redirect settings: 160.0.0.2:3123 is redirected to 9.2.36.253:80
Default web traffic statistics:
  Input Bytes = 8, Input Packets = 186
  Output Bytes = 6, Output Packets = 154

```

The **show ssg host** command can also be used to display the server to which web traffic is redirected when a user logs in to a service that is configured with attribute `ssg-service-info=KWserver-group-name` or attribute `ssg-service-info=KW0`.

```

Router# show ssg host 1.6.6.2
.
.
.
User has permanent web-redirect settings: 160.0.0.2:3123 is redirected to 9.2.36.246:80

```

When attribute `26,9,251,KW0` is configured, the **show ssg host** command will show that the user's web traffic is not redirected, as in the following example:

```

Router# show ssg host 1.6.6.2
.
.
.
User has permanent web-redirect settings: 160.0.0.2:3123 is redirected to 0.0.0.0:0

```

show ssg connection Sample Output: Example

Use the **show ssg connection** command to display connection information for a specific host and service when the 26,9,251,KW`server-group-name` attribute is configured in the service profile for the service.

In the example that follows, a sample configuration is provided along with the corresponding **show ssg connection** command output. The attribute `ssg-service-info = KWservice_http_proxy_isp_a` must be configured in the service profile.

```
!
server-group service_http_proxy_isp_a
  server 9.2.36.246 80
```

The following output corresponds to the sample configuration above:

```
Router# show ssg connection 1.6.6.2 internet_isp_a
.
.
.
      Input Bytes = 16, Input Packets = 234
      Output Bytes = 11, Output Packets = 198
```

Additional References

The following sections provide references related to SSG permanent TCP redirection.

Related Documents

Related Topic	Document Title
SSG commands	<i>Cisco IOS Wide-Area Networking Command Reference</i> , Release 12.3 T
SSG configuration tasks	<i>Service Selection Gateway</i> , Release 12.3(4)T new-feature document <i>SSG TCP Redirect for Services</i> , Release 12.2(13)T new-feature document
SESM	<i>Cisco Subscriber Edge Services Manager</i> <i>Cisco Service Selection Dashboard</i>
RADIUS commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T
RADIUS configuration tasks	<i>Cisco IOS Security Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature. Support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature. Support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature. Support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents the new [Glossary](#) command.

redirect permanent http to

To configure 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.
<i>server-group</i>	Server group name to which HTTP traffic will be sent.

Defaults

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.

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 10.76.86.90 80
 !
 server-group auth_web_group
   server 9.2.36.253 80
 !
 server-group unauth_web_group
   server 9.2.76.12 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.



Glossary

hot spot—A specific geographic location in which an access point provides public wireless broadband network services to mobile visitors through a wireless LAN (WLAN). Examples of hot spots include airports, coffee shops, hotels, and conference centers. Hot spots typically have a short range of access.

HTTP proxy server—A server that acts like an HTTP (or web) server for the user, but is just a proxy. Browsers such as Netscape, Mozilla, and Windows Internet Explorer can be configured to send all HTTP traffic to the HTTP proxy server, which brings back the web pages from the real HTTP server.

traffic—In this document, refers to HTTP traffic from the HTTP-proxy user. Note that this traffic would always be destined for the HTTP proxy server that is configured in the user's browser.

user (or HTTP proxy user)—In this document, refers to a user with HTTP proxy settings in his browser (unless otherwise stated).

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

