Configuring SSG Subscriber Experience Features

First Published: May 1, 2005
Last Updated: October 2, 2009

Note Effective with Cisco IOS Release 15.0(1)M, this feature is not available in Cisco IOS software.

This chapter provides information about configuring the following Service Selection Gateway (SSG) subscriber experience features:

- Hierarchical Policing
- TCP Redirection
- Per-Session Firewall
- DNS Redirection

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Configuring SSG Subscriber Experience Features" section on page 49.

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

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

Contents

- Prerequisites for Configuring SSG Subscriber Experience Features, page 2
- Information About SSG Subscriber Experience Features, page 2
- How to Configure SSG Subscriber Experience Features, page 18
- Configuration Examples for Configuring SSG Subscriber Experience Features, page 43
- Additional References, page 47
- Feature Information for Configuring SSG Subscriber Experience Features, page 49

Prerequisites for Configuring SSG Subscriber Experience Features

Before you can perform the tasks in this process, you must enable SSG. See the *Cisco IOS Security Configuration Guide, Release 12.4*. Refer to Implementing SSG: Initial Tasks.

Information About SSG Subscriber Experience Features

With SSG subscriber experience features, an internet service provider (ISP) can configure SSG features to suit individual user preferences and to control the user experience for its subscribers.

For example, SSG allows users to choose multiple services that have their own specific bandwidth requirements (such as an ISP's regular service or a premium service). To ensure that the bandwidth is distributed properly for customers who use different types of services, SSG uses traffic policing. Furthermore, because the bandwidth can be first policed between users, and then policed again between the services to a particular user (a hierarchical policing technique), SSG provides the SSG Hierarchical Policing feature, which can be configured to suit particular user requirements.

The SSG Hierarchical Policing feature is just one of the SSG subscriber experience features described in this chapter. The remainder of this chapter provides all the information required to configure SSG subscriber experience features, based on user preferences.

This section provides conceptual information and restrictions that may apply to specific SSG subscriber experience features.

For detailed information about configuring SSG subscriber experience features, see How to Configure SSG Subscriber Experience Features, page 18.

Before you configure SSG subscriber experience features, review and understand the SSG concepts provided in the following sections:

- SSG Hierarchical Policing Overview, page 3
- SSG TCP Redirect Features Overview, page 6
- Per-Session Firewall Overview, page 13
- Default DNS Redirection Overview, page 15

SSG Hierarchical Policing Overview

SSG allows subscribers to choose one or more types of services. Each type of service has its own bandwidth requirements; for example, suppose an ISP has two types of services, regular and premium. The regular service is cheaper for customers but is allocated less bandwidth per customer than the premium service, which provides more bandwidth and a higher quality connection than the regular service. SSG, therefore, requires a mechanism to ensure that bandwidth is distributed properly for customers using different types of services.

The following sections explain the concepts of hierarchical policing:

- SSG Per-User and Per-Session Policing, page 3
- SSG Hierarchical Policing Token Bucket Scheme, page 3

For detailed information about configuring SSG hierarchical policing, see Configuring SSG Hierarchical Policing, page 18.

SSG Per-User and Per-Session Policing

Traffic policing is the concept of limiting the transmission rate of traffic entering or leaving a node. In SSG, traffic policing can be used to allocate bandwidth between subscribers and between services to a particular subscriber to ensure that all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-session policing to ensure that bandwidth is distributed properly between subscribers (per-user policing) and between services to a particular subscriber (per-session policing). Because these policing techniques are hierarchical in nature (bandwidth can be first policed between users and then policed again between services to a particular user), this complete feature is called SSG Hierarchical Policing.

- Per-user policing:
  - is used to police the aggregated traffic that is destined to or that is sent from a particular subscriber and can police only the bandwidth allocated to a subscriber.
  - cannot identify services to a particular subscriber and police bandwidth between these services.
- Per-session policing:
  - is used to police the types of services available to a subscriber.
  - provides a mechanism for identifying the types of services (such as video service or Internet access in the example) and ensuring that users do not exceed the allocated bandwidth for the service.
  - is useful when an SSG subscriber subscribes to more than one service, and multiple services are allocated different amounts of bandwidth; for example, suppose a single subscriber pays separately for Internet access and video service but receives both services from the same service provider. The video service is allocated more bandwidth than the Internet access service and costs more to the subscriber.

SSG Hierarchical Policing Token Bucket Scheme

The SSG Hierarchical Policing token bucket scheme polices the use of bandwidth through an algorithm. The parameters used by the algorithm to allocate bandwidth are user configurable; however, other unpredictable variables, such as time between packets and packet sizes, ultimately determine whether a packet is transmitted or dropped.

The following sections explain the aspects of the SSG Hierarchical Policing token bucket scheme:

- Committed Rate, Normal Burst, and Excess Burst
- Actual and Compound Debt
- Token Bucket Algorithm Calculations

Committed Rate, Normal Burst, and Excess Burst

The SSG Hierarchical Policing feature limits the transmission rate of traffic based on a token bucket algorithm that analyzes a packet and determines whether the packet should be forwarded to its destination or dropped. A token bucket can be used to monitor upstream traffic (traffic sent by a subscriber) or downstream traffic (traffic destined for a subscriber), and a bucket can be configured in both directions for a user or a service profile.

As shown in Table 1, the committed rate, normal burst, and excess-burst are the user-configurable parameters when configuring SSG Hierarchical Policing. These parameters are used by the SSG Hierarchical Policing token buckets to evaluate traffic.

Table 1 SSG Hierarchical Policing User-Configurable Parameters

Parameter	Purpose
committed-rate	The committed-rate parameter is the amount of bandwidth that is entitled to a subscriber (per-user policing) or to a service for a particular subscriber (per-session policing). The token bucket algorithm uses the committed-rate parameter for generating tokens when a packet arrives. The committed-rate parameter is equal to the minimum amount of bandwidth that is guaranteed to a subscriber or service. **Note** The committed rate is specified in bits per second, while the normal burst and excess-burst sizes are specified in bytes.
normal-burst	The normal-burst parameter determines the maximum size of a traffic burst before packets are dropped.
excess-burst	The excess-burst size parameter is an optional variable that determines the burst size beyond which all traffic is dropped. The excess-burst size parameter is disabled when it is set lower than the normal burst size. If the excess-burst size parameter is configured, the traffic that falls between the normal-burst size and the excess-burst sizes is dropped based on a calculated probability (the probability that traffic will be forwarded increases as the size of the configured excess-burst parameter increases). If a token bucket is configured with an excess-burst size, subscribers and services using additional bandwidth will likely experience sporadic drops (similar to the method in which packets are dropped by using the Random Early Detection [RED] feature).

Actual and Compound Debt

Before explaining the calculations used by the token bucket algorithm to drop or forward packets, an understanding of actual and compound debt is useful.

When a normal or excess-burst is required to forward traffic, debt is incurred. The debt is then compared to the configured parameters, and the algorithm either sends or drops the packet based on the comparison.

The probability for the algorithm to forward large packets increases when a user or a service has been idle for a long period of time.

Table 2 provides a definition of actual and compound debt:

Table 2 Actual and Compound Debt Definitions

Term	Definition
actual debt	The actual debt is the number of tokens that have been borrowed by the current packet. When a packet is forwarded by using a burst, the actual debt is compared to the user-configured normal-burst size. If the actual debt is less than the normal-burst size, the packet is forwarded. If the actual debt is greater than the normal-burst size, the packet is either dropped (excess-burst configuration is less than the normal-burst size) or forwarded by using the excess-burst size (which is possible when the excess-burst size is larger than the normal-burst size).
compound debt	The compound debt is equal to the total number of tokens that have been borrowed—in addition to the normal-burst allowance. Because additional tokens cannot be borrowed when the excess-burst parameter is not set, compound debt is only used when the excess-burst parameter is set. Compound debt is only a factor in forwarding a packet after the actual debt exceeds the normal-burst size. Compound debt is compared to the excess-burst size. If the compound debt is less than the excess-burst size, the packet is forwarded. If the compound debt is greater than the excess-burst size, the packet is dropped.

Token Bucket Algorithm Calculations

The following steps describe how the algorithm that polices traffic operates:

1. The packet arrives. The packet size (Ps) is noted.
2. The time between the arrival of the last packet and the arrival of the current packet is calculated. This calculation is called time difference (td).
3. The actual debt is calculated and is based on the following formula:

   actual_debt = previous_actual_debt (Ad) + Ps
4. The tokens that can be generated by the arriving packet are calculated:

   tokens = committed_rate (Ar) * td
5. The tokens are then compared to the actual debt.
   a. If tokens > actual_debt, the actual debt for the packet is set at 0.
   b. If tokens < actual debt, the actual debt is calculated by using the following formula:

      actual_debt = actual_debt – tokens
6. The actual debt is compared to the normal burst to see if traffic should be forwarded or dropped.

a. If actual_debt < normal_burst, the packet conforms and is forwarded.

b. If actual_debt > normal_burst, the packet is dropped if the excess-burst size is not configured. If actual_debt > normal_burst and the excess-burst size is configured, compound debt is checked.

c. The compound debt is calculated by using the following formula:

   compound_debt = previous_compound_debt + (actual_debt – normal_burst)

d. If compound_debt < excess_burst, the packet is forwarded.

e. If compound_debt > excess_burst, the packet is dropped.

SSG TCP Redirect Features Overview

The SSG TCP Redirect function includes a suite of features that are described in the following sections:

- SSG TCP Redirect for Services Overview, page 6
- SSG TCP Redirect for Unauthenticated Users, page 6
- SSG TCP Redirect for Unauthorized Services, page 7
- SSG TCP Redirect Initial Captivation, page 8
- SSG TCP Redirect Access Control Lists Overview, page 9
- SSG Permanent TCP Redirection Overview, page 10

For detailed information about configuring TCP Redirect features, see Configuring SSG TCP Redirection Features, page 22.

SSG TCP Redirect for Services Overview

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 login window. Similarly, if users try to access a service to which they have not logged in, the packets are redirected to a captive portal that can provide a service login window.

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 login window when they start a browser session. In SESM Release 3.1(3), captive portal applications can also redirect users to a service login window, 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

SSG TCP Redirect for Unauthenticated Users

The SSG TCP Redirect for Unauthenticated Users feature redirects packets from a user if the user has not been authorized by the service provider. When an unauthorized subscriber attempts to connect to a service on a TCP port (for example, to www.cisco.com), the SSG TCP Redirect feature redirects the packet to the captive portal (SESM or a group of SESM devices). SESM issues a redirect to the browser

to display the login window. The subscriber logs in to SESM and is authenticated and authorized. SESM then presents the subscriber with a personalized home page, the service provider home page, or the original URL.

The SSG TCP Redirect for Services feature always sends redirected packets 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. For upstream packets, SSG modifies the destination IP address and TCP port to reflect the destination captive portal. For downstream packets, SSG returns the source IP address and port to the original packet's destination. SSG uses the same redirect server if multiple TCP sessions from the same user are redirected. When the TCP session terminates or is idle for more than 60 seconds, SSG clears translations of packets made before the packets are sent to the captive portal. In host-key mode with overlapping user IP addresses, redirection works only for host-keyed servers.

Note This feature applies only to non-PPP users. PPP users are always authenticated as part of the PPP negotiation process. PPP users logging off from SESM are also redirected.

SSG tracks the list of interesting ports for unauthenticated and authenticated users based on the redirect configurations. The list of interesting ports is built each time the redirect configuration changes, but this does not impact the performance of SSG as the ports are built during the configuration.

The following describes the behavior of redirection for unauthorized users:

- If a user is subject to redirection or captivation, then packets from the user that match the protocol and ports configured as the redirection and captivation filter are sent to SESM. If the user packet does not match the filter, SSG drops the packet.
- SSG drops all packets to the user, unless the packet arrives from the SESM or the Open Garden network.

SSG TCP Redirect for Unauthorized Services

The Redirect for Unauthorized Services feature redirects TCP sessions from authenticated users who have not been authorized to access service networks. SSG TCP Redirect redirects the packets to a captive portal, such as SESM, which then prompts the user to log in.

SSG can redirect unauthorized TCP sessions for different networks to different servers. For network-based redirection, a list of networks are used for unauthorized service redirect. The network list is associated with a group of servers. Only one network list can be associated with a server group.

The server group can also be associated with a port or a list of ports. Servers handle particular captive portal applications as defined by the port that they use. TCP sessions redirected to servers can be restricted based on a port or port list. A port list defines a named list of interesting destination TCP ports. The port list is associated with a server group and is used to restrict the applications redirected to a server group. Only one port list or port can be associated with a server group.

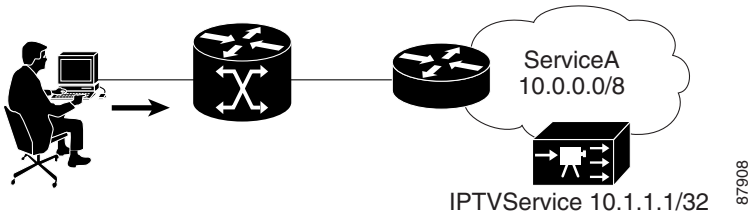
Note Users will not be redirected to the unauthorized service SESM, if the destination port is not listed in any of the port lists. You need to configure the destination ports in a port list and redirect the port list to an unauthorized service SESM for this to work.

If none of the destination networks matches the networks in the network list, you can set up a default server group to receive redirected packets by using the **redirect unauthorized-service** command.

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

SSG TCP Redirect also restricts access to certain networks that are part of another authorized service. For example, in Figure 1 the user is allowed to access ServiceA. IPTVService is part of ServiceA, but the user is not authorized to access IPTVService. SSG redirects TCP sessions from the user to IPTVService (10.1.1.1/32), but allows access to anywhere else in ServiceA (10.0.0.0/8).

Figure 1 Restricting Access to Networks Within Authorized Services



The following describes the behavior of redirection for unauthorized services:

- If a packet arrives from an unauthorized SSG user or a packet is destined to an unauthorized service, SSG redirects the packet if the packet matches the protocol and ports configured as the redirection filter. If the packet does not match the filter, SSG drops the packet.
- If a packet arrives from an unauthorized service or is destined to an unauthorized SSG user, SSG drops the packet.
- If a user's connection is subject to redirection or captivation, any packets from the connection that match the protocol and ports for redirection and captivation are redirected to SESM by SSG.
- If packets from the connection do not match the protocol and ports configured as a filter, SSG drops the packets.

SSG TCP Redirect Initial Captivation

The SSG TCP Redirect Initial Captivation feature redirects certain packets from users for a specific period of time. After a user logs in, packets to certain TCP ports are redirected to a server for advertisements and branding. The initial captivation feature redirects all user packets to those TCP ports regardless of the destination address, and is active for a specified duration, starting from the first redirected session.

If you configure the initial captivation feature globally by using the CLI, the configuration applies to all authenticated users. You can also enable the initial captivation feature in the RADIUS user profile as an Account-Info attribute to override the CLI setting.

The user profile contains the following information for initial captivation:

- Server group name

Note Use the CLI to configure the server group and to associate a port or port list to the server group.

- Duration of captivation
- Service name (optional)

Note If you specify the optional service name, captivation is activated only when a user logs in to that service.

Typically, if a service is connected, SSG forwards packets to a user and packets from a user even if the packets do not match the protocol and TCP ports that are specified for redirection. However, the behavior of initial captivation on the Cisco 10000 series router differs in the following ways:

- When a packet arrives from an SSG user and the packet matches the protocol and TCP ports configured as the redirection filter, the packet is subject to initial captivation and is redirected. If the packet does not match the redirection filter, it is not subject to initial captivation and the packet is dropped.
- When a packet arrives from a service destined for an SSG user who is subject to initial captivation, the packet is dropped.

SSG TCP Redirect Access Control Lists Overview

SSG TCP redirect functionality allows SSG to redirect TCP packets from users on the basis of the destination port number. The SSG TCP Redirect Access Control Lists feature enables SSG to use Cisco IOS software access control lists (ACLs or access lists) to select Internet traffic for redirection. An ACL is associated with a TCP redirect server group. A TCP packet from a subscriber is redirected to a server in that group only if permitted by the access list for that group. This functionality can be used for all types of redirections: unauthenticated users, unauthorized service, initial and periodic captivation, prepaid redirection on quota expiry, and Simple Mail Transfer Protocol (SMTP) forwarding.

An ACL:

- is an additional, optional criterion for selecting packets for redirection.
- makes a port or port list optional.
  - If a port list is also associated with a server group, the TCP packet must match the ACL and port list.
  - Only one ACL can be associated with a server group.

    Either an ACL, or a port or port list should be configured with server groups for unauthorized service redirection and captivation. The ACL can be simple or extended, and can also be named or numbered.

SSG provides an option to configure a default ACL for TCP redirections. This default is used with server groups that do not have a configured ACL.

This section describes the following SSG TCP Redirect ACL concepts:

- Uses for SSG TCP Redirect Access Control Lists, page 9
- Prevention of Redirection of Non-HTTP Applications, page 10
- Location-Based Redirections, page 10
- Redirection to a Service Network for Captivation, page 10
- Redirection for a Range of TCP Ports, page 10

For information about configuring SSG TCP redirect ACLs, see Associating an Access Control List with a Redirection Group, page 26.

Uses for SSG TCP Redirect Access Control Lists

The SSG TCP Redirect Access Control Lists feature allows you to use access lists to select TCP traffic sessions for redirection or to prevent certain TCP traffic sessions from being redirected.

The following are examples of possible uses of this feature.

Prevention of Redirection of Non-HTTP Applications

Ports or port lists can be used with the SSG TCP Redirect feature to control which applications are redirected; however, some servers may provide non-HTTP application services on standard ports. The TCP redirection servers may not be able to handle such applications. In these cases, ACLs can be used to prevent redirection of TCP sessions to these types of application servers.

Location-Based Redirections

SSG TCP redirect ACLs can be used for location-based redirections. For example, a network might include multiple SESMs, each of which is customized for a different location. SSG can be configured with each SESM in a different TCP redirect group. Each TCP redirect group can be associated with an ACL that permits a particular subnet of hosts from one location. The server groups can then be used for location-based unauthenticated user or service redirections.

Redirection to a Service Network for Captivation

For captivation redirections, the messaging portal is used to redirect browsers to a different URL on advertising servers. When captivation is active and the advertising servers are outside the SSG default network and open gardens, the TCP session to such servers is redirected back to the messaging portal, resulting in a loop. The SSG TCP Redirect Access Control Lists feature can be used to prevent redirection of traffic to advertisement servers for captivation.

Redirection for a Range of TCP Ports

Cisco IOS software extended ACLs provide the option to configure a range of ports in an ACL entry. Extended ACLs can be used with the SSG TCP Redirect feature for redirection on the basis of a range of ports, without having to enter all the ports in the range into a port list.

SSG Permanent TCP Redirection Overview

The SSG Permanent TCP Redirection feature enables Service Selection Gateway (SSG), 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.

This section describes the following SSG Permanent TCP Redirection concepts:

- How SSG Permanent TCP Redirection Works
- Supported SSG Permanent TCP Redirection Functionality
- RADIUS Attributes for SSG Permanent TCP Redirection

How SSG Permanent TCP Redirection Works

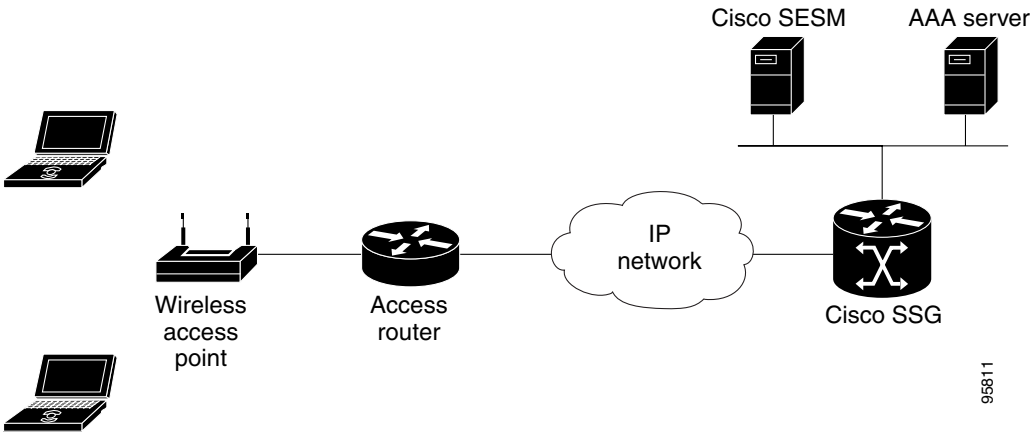
An HTTP-proxy server is a server that acts like an HTTP (or web) server for the user, but is just a proxy. Browsers such as Netscape, Mozilla, and Windows Internet Explorer can be configured to send all HTTP traffic to an HTTP proxy server, which brings back the web pages from the real HTTP server. In this document, the term *traffic* refers to HTTP traffic from the HTTP proxy user, and the term *user* (or HTTP proxy user) refers to a user with HTTP proxy settings in his or her browser (unless otherwise stated).

When an HTTP proxy server is configured in a browser, HTTP traffic is always directed to the HTTP proxy server. HTTP proxy servers are usually internal to a corporate intranet or Internet service provider (ISP) and are usually not routable globally.

If an HTTP proxy user attempts to open a web page from a public wireless LAN (PWLAN), SSG drops the HTTP traffic because the HTTP server is not routable by SSG. The SSG Permanent TCP Redirection feature enables SSG to support users whose web browsers are configured with HTTP proxy servers.

Figure 2 shows an example of a typical wireless LAN (WLAN) topology that uses permanent TCP redirection.

Figure 2 Sample WLAN Topology for SSG Permanent TCP Redirection



The following steps provide a general description of how permanent TCP redirection works:

1. A user (IP*u*) enters a WLAN hot spot (a specific location in which an access point provides public wireless broadband network services to mobile visitors) and opens the browser on his or her laptop. The browser is configured with an HTTP-proxy server (IP*w* : Port*w*).
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 (IP*w* : Portw).
3. SSG intercepts the traffic from unauthenticated user IP*u* and passes the traffic 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, the SESM captive portal sends a message to SSG containing the user's HTTP proxy settings.
5. SSG stores the information (namely, that user IP*u* has the HTTP proxy server setting IP*w* : Port*w*). From now on, SSG will redirect all traffic from user IP*u* and destined for IP*w* : Port*w* 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 IP*u* and destined for IP*w* : Port*w* 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 allows users with browsers that are configured with HTTP proxy servers to log in and connect to 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. SSG redirects the users to the SESM captive portal by 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 allows users to initiate an end-to-end Virtual Private Network (VPN) connection after users have 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 off 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 accounting includes all HTTP traffic going to the HTTP proxy server, including the 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 3 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 3 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	KW*server-group-name*—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. `Example: ssg-service-info = KWhttp-proxy-isp_a`
26	9	251	Service-Info	KW0—When a user logs in to the service, SSG allows all HTTP traffic to go to the service, without redirection, as if there are no HTTP-proxy server settings in the user's browser. **Note** The service network entries must include the actual HTTP proxy address. This subattribute takes precedence over the 26,9,251 KW*server-group-name* attribute. `Example: ssg-service-info = KW0`

Per-Session Firewall Overview

SSG uses Cisco IOS software access control lists (ACLs) to prevent users, services, and pass-through traffic from accessing specific IP addresses and ports. This process is commonly referred to as a per-session firewall.

Note Certain restrictions apply when using per-session firewalls for SSG. see Restrictions for Per-Session Firewall, page 15, before configuring Per-Session firewalls.

This section describes the following SSG per-session firewall concepts:

- Access List Attributes for User and Service Profiles, page 13
- Downstream Access Control List Attribute—outacl, page 14
- Upstream Access Control List Attribute—inacl, page 14
- Restrictions for Per-Session Firewall, page 15

For detailed information about configuring per-session firewalls for SSG, see Configuring a Per-Session Firewall, page 40.

Access List Attributes for User and Service Profiles

When an ACL attribute is added to a service profile, all users of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

When an ACL attribute is added to a user profile, the attribute applies globally to all traffic for the user. Transparent pass-through Upstream and Downstream attributes, including the Upstream Access Control List and Downstream Access Control List attributes, can be added to a special pseudo-service profile that can be downloaded to SSG from a RADIUS server. Additionally, locally configured ACLs can be used. After the ACLs have been defined, they are applied to all traffic passed by the transparent pass-through feature.

User profiles define the services and service groups to which a user is subscribed. RADIUS user profiles contain a password, a list of subscribed services and groups, ACLs, and timeouts. User profiles are configured on the RADIUS server or directly on the router. The RADIUS server or SESM downloads the user profiles to the router.

Downstream Access Control List Attribute—outacl

The following Cisco-AV pair attribute specifies either a Cisco IOS software standard ACL or an extended ACL to be applied to downstream traffic going to the user.

Cisco-AVpair = "ip:outacl[**#***number*]**=**{*standard-access-control-list* | *extended-access-control-list*}**"**

Syntax Description

number	Access list identifier.
standard-access-control-list	Standard access control list.
extended-access-control-list	Extended access control list.

Example

```
Cisco-AVpair = "ip:outacl#101=deny tcp 10.168.1.0 0.0.0.255 any eq 21"
```

Note Multiple instances of the Downstream Access Control List attribute can occur within a single profile. Use one attribute for each ACL statement. You can use multiple attributes for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

Upstream Access Control List Attribute—inacl

The following Cisco-AV pair attribute specifies either a Cisco IOS software standard ACL or an extended ACL to be applied to upstream traffic coming from the user.

Cisco-AVpair = "ip:inacl[**#***number*]**=**{*standard-access-control-list* | *extended-access-control-list*}**"**

Syntax Description

number	Access list identifier.
standard-access-control-list	Standard access control list.
extended-access-control-list	Extended access control list.

Example

```
Cisco-AVpair = "ip:inacl#101=deny tcp 10.168.1.0 0.0.0.255 any eq 21"
```

Note Multiple instances of the Upstream Access Control List attribute can occur within a single profile. Use one attribute for each access control list statement. You can use multiple attributes for the same ACL. Multiple attributes are downloaded according to the number specified and are executed in that order.

Restrictions for Per-Session Firewall

Per-Session Firewall for SSG has the following restrictions:

- SSG accepts only the permit and deny actions for a per-user ACL. You can place ACLs on user traffic for both the input and output directions that are similar to existing Cisco IOS software ACLs; however, the **log** option is not accepted.
- SSG supports mini-ACLs with eight or less access control entries (ACEs), which can be extended ACEs.
- SSG does not support turbo ACLs applied to SSG users. Turbo ACLs have more than eight ACEs defined.
- To support some SSG features, SSG prepends ACEs on user ACLs. Because the number of ACEs is restricted to a maximum of eight, the number of ACEs that you can define is therefore reduced in some cases. For example, for the Port-Bundle Host Key feature, an ACE is required on both the host input and output ACL. This allows seven ACEs that you can define.
- SSG does not support the ability to apply per-service (connection level) ACLs. ACLs for QoS classification are not applicable to SSG host interfaces.
- SSG ACLs take precedence over Cisco IOS software ACLs. If you configure a Cisco IOS software ACL on an SSG interface by using the **ip access-group** command, the router applies the ACL as long as an SSG ACL is not applied to the interface in the same direction. If an SSG ACL is applied to the interface in the same direction, the router applies the SSG ACL.

Default DNS Redirection Overview

SSG default DNS redirection allows a default Domain Name System (DNS) domain to be configured in a service profile. When a default DNS domain is configured in a service profile, all DNS queries that do not match a domain name are redirected to the DNS server for that service.

This section describes the following DNS redirection concepts:

- DNS Redirection for Unauthenticated Users, page 15
- SSG Domain Name Vendor-Specific Attribute, page 16
- Restrictions for Dynamic DNS Assignment, page 17

For detailed information about configuring default DNS redirection, see Configuring Default DNS Redirection, page 41.

DNS Redirection for Unauthenticated Users

The default domain can be configured to apply to DNS queries from unauthenticated users only. This type of configuration enables SSG to redirect all DNS queries for unauthenticated users to the Cisco Subscriber Edge Services Manager (SESM) DNS server, which can spoof the responses if required.

A domain name within the question section of the DNS packet is compared in sequence in the upstream path.

The sequence is as follows:

1. Domain names are configured in the logged-in services. If a match is found, the request is redirected to the DNS server for the matched service.
2. Domain names are configured in the open garden service. If a match is found, the request is redirected to the DNS server for the open garden service.
3. Default DNS domains are defined as an asterisk [*] in logged-in and in open garden services.
4. If the user is logged in to a service that has Internet connectivity, the request is redirected to the first service in the user's service access order list that has Internet connectivity, which is defined as access to a service containing a Service Route attribute of 0.0.0.0/0.
5. If there is an open garden Internet service, the request is redirected to this service.
6. If a match is not found until now, the request is forwarded to the DNS server defined in the client's TCP/IP stack.

Default DNS redirection is useful in a public wireless LAN (PWLAN) environment in which a user's browser may be configured with a home page that is part of a corporate internal network. Since the home page domain will never be resolved by a DNS server in the Internet, the TCP session from the user will never be initiated. Default DNS redirection allows SSG to redirect all DNS queries to a DNS server that can resolve all queries—for example, the DNS server on the Cisco Subscriber Edge Services Manager (SESM), which can spoof all unresolved DNS queries.

SSG Domain Name Vendor-Specific Attribute

Table 4 describes the Domain Name vendor-specific attribute (VSA) used by SSG. The Domain Name VSA specifies domain names that get DNS resolution from the DNS servers specified in the DNS server address.

Table 4 SSG Vendor-Specific Attribute for Domain Name

Attribute ID	Vendor ID	Subattribute ID and Type	Subattribute Name	Subattribute Data

26	9	251 Service-Info	Domain Name	O{*name1*[;*name2*]...[;*nameX*] | *[;unauthenticated]}
				name1—Domain name that gets DNS resolution from this server.
				name2...x—Additional domain names that get DNS resolution from this server.
				*—Default domain for all DNS queries. Note that this cannot be part of a list of domain names.
				*O;unauthenticated—Default domain that applies to DNS queries for unauthenticated users only. This is useful in a wireless LAN environment in which SSG redirects all DNS queries for unauthenticated users to the SESM DNS server, which can spoof the responses if required.
				Example:
				`ssg-service-info = "Ocisco.com;cisco-sales.com"`
				Example:
				`ssg-service-info = "O*;unauthenticated"`

Restrictions for Dynamic DNS Assignment

When the DNS redirection server is statically configured in the service profile with SSG attributes, the following restrictions apply:

- For mobile deployments, the mobile operator must configure ISP DNS addresses for users to connect to.
- For any given service, after the attributes are downloaded, they are applied to all connections for that service. This is not a restriction for proxy or dial-in tunnel services (where all users are usually assigned the same DNS addresses). However, for L2TP dial-out tunnel cases, the same tunnel can be used to connect to different ISPs, and thus different DNS addresses may be required.

These DNS redirections can now be dynamically assigned on a per-connection basis for proxy and tunnel services. This is achieved by negotiation of the DNS addresses during authentication to the proxy or tunnel service.

For all service connections, SSG is capable of learning the DNS addresses on a per-connection basis. Any DNS addresses discovered in this way override DNS addresses that are statically configured in the service profile. The mechanisms employed for discovering these DNS addresses are described in Cisco-AVpair Attributes, page 18.

Cisco-AVpair Attributes

The Cisco-AVpair attributes are used in user and service profiles to configure ACLs and L2TP.

Table 5 lists the Cisco-AVpair attributes.

Table 5 Cisco-AVPair Attributes

Attribute	Description
Downstream Access Control List (outacl)	Specifies either a Cisco IOS software standard ACL or an extended ACL to be applied to downstream traffic going to the user.
L2TP Tunnel Password	Specifies the secret (the password) used for L2TP tunnel authentication.
Upstream Access Control List (inacl)	Specifies either a Cisco IOS software standard ACL or an extended ACL to be applied to upstream traffic coming from the user.
VPDN IP Address	Specifies the IP addresses of the home gateways (LNSes) to receive the L2TP connections.
VPDN Tunnel ID	Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.

How to Configure SSG Subscriber Experience Features

This section contains the following tasks:

- Configuring SSG Hierarchical Policing, page 18
- Configuring SSG TCP Redirection Features, page 22
- Configuring a Per-Session Firewall, page 40
- Configuring Default DNS Redirection, page 41

For conceptual information about SSG subscriber experience features, see Information About SSG Subscriber Experience Features, page 2.

Configuring SSG Hierarchical Policing

Perform the following tasks to configure SSG hierarchical policing:

- Configuring a RADIUS User Profile for Per-User Policing, page 18
- Configuring SSG Hierarchical Policing in a RADIUS Service Profile, page 19
- Enabling SSG Hierarchical Policing on the Router, page 20
- Troubleshooting SSG Hierarchical Policing, page 21

For conceptual information about SSG hierarchical policing, see SSG Hierarchical Policing Overview, page 3.

Configuring a RADIUS User Profile for Per-User Policing

To accommodate per-user policing, modify the subscriber user profile to define the average bandwidth that the user is entitled to obtain, and the normal and excess-burst tolerance that the user can have.

To configure a RADIUS user profile for per-user policing, add the following attribute to the user profile:

Account-Info = "**QU**;*upstream-bandwidth*;*upstream-normal-burst*;[*upstream-excess-burst*];**D**;*downstream-bandwidth*;*downstream-normal-burst*;[*downstream-excess-burst*]"

Example

Account-Info = **"QU;**80000**;**40000**;**50000**;D;**80000**;**40000**;**50000**"**

Note For details on how to modify a RADIUS user profile, see your RADIUS server documentation.

Configuring SSG Hierarchical Policing in a RADIUS Service Profile

For per-session policing, the RADIUS service profile (which can be configured in a remote AAA server or locally, on the router) has to be modified to accommodate SSG Hierarchical Policing. The service profile defines the average rate a service has to achieve and the normal and excess-burst size the service can tolerate to provide corresponding quality of service.

Modifying the RADIUS Service Profile on the AAA Server

To configure a service profile for per-session policing on the AAA server, add the following attribute to the service profile:

Service-Info = "**QU**;*upstream-token-rate*;*upstream-normal-burst*;[*upstream-excess-burst*];**D**;*downstream-token-rate*;*downstream-normal-burst*;[*downstream-excess-burst*]"

Example

Service-Info = **"QU;**40000**;**20000**;**25000**;D;**40000**;**20000**;**25000**"**

Note For details on how to modify a service profile for per-session policing on the AAA server, see your AAA server documentation.

Modifying the RADIUS Service Profile Locally on the Router

To configure a service profile with all of the policing parameters locally on the router, enter the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **local-profile** *profile-name*
4. **attribute** *radius-attribute-id vendor-id cisco-vsa-type* **"QU;***upstream-token-rate***;***upstream-normal-burst***;**[*upstream-excess-burst*];**D**;*downstream-token-rate***;***downstream-normal-burst***;***downstream-excess-burst***"**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`local-profile`** *`profile-name`* **Example:** `Router(config)# local-profile profile-2065`	Enters profile configuration mode. Configures a local RADIUS service profile.
Step 4	**`attribute`** *`radius-attribute-id vendor-id cisco-vsa-type`* **`"QU;`***`upstream-token-rate`***`;`***`upstream-normal-burst`***`;`** [*`upstream-excess-burst`*]**`;D;`***`downstream-token-rate`***`;`***`downstream-normal-burst`***`;`***`downstream-excess-burst`***`"`** **Example:** `Router(config-prof)# attribute 26 9 251"QU;80000;40000; 50000;D;downstream-token-rate;40000;50000"`	Configures the policing attributes in a local RADIUS service profile. The **Q** parameter (as shown in the command) represents QoS. The variables are used to configure upstream (**U**) and downstream (**D**) policing. The upstream traffic is the traffic that travels from the subscriber to the network, while the downstream traffic is the traffic that travels from the network to the subscriber. SSG Hierarchical Policing can be configured in either direction or in both directions simultaneously.

Enabling SSG Hierarchical Policing on the Router

After you configure the SSG hierarchical policing parameters in the user or service profile, enter the **ssg qos police** command on the router to enable per-user or per-session policing.

Note To disable SSG Hierarchical Policing on a router, use the **no ssg qos police user** and the **no ssg qos police session** commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg qos police user**
4. **ssg qos police session**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg qos police user** **Example:** `Router(config)# ssg qos police user`	Enables SSG per-user policing on the router.
Step 4	**ssg qos police session** **Example:** `Router(config)# ssg qos police session`	Enables SSG per-session policing.

Troubleshooting SSG Hierarchical Policing

Use the following commands to troubleshoot the SSG Hierarchical Policing feature:

SUMMARY STEPS

1. **show ssg host**
2. **show ssg connection**
3. **debug ssg data**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ssg host** **Example:** `Router# show ssg host`	Displays information about an SSG host, including whether policing is enabled or disabled and the policing configurations of a particular host. Use the **show ssg host** command to verify per-user policing.
Step 2	**show ssg connection** **Example:** `Router# show ssg connection`	Displays information about a particular SSG connection, including the policing parameters.
Step 3	**debug ssg data** **Example:** `Router# debug ssg data`	Displays SSG QoS information.

Configuring SSG TCP Redirection Features

This section describes how to configure SSG TCP Redirection features that allow SSG to redirect TCP packets, based on the destination port number.

For conceptual information about SSG TCP Redirection features, see SSG TCP Redirect Features Overview, page 6.

Note Before you can perform the tasks in this process, you must enable SSG. See the *Cisco IOS Security Configuration Guide, Release 12.4*. Refer to *Implementing SSG: Initial Tasks.*

Perform the following tasks to configure TCP redirection features:

- Enabling SSG TCP Redirect for Services (Required), page 22
- Defining a Captive Portal Group, page 24
- Configuring Initial and Periodic Captivation, page 25
- Associating an Access Control List with a Redirection Group, page 26
- Verifying SSG TCP Redirect Access Control Lists, page 28
- Configuring TCP Redirection of Unauthenticated Subscribers, page 29
- Configuring TCP Ports for Redirection, page 30
- Configuring Unauthorized Service Redirection, page 32
- Configuring SMTP Redirection, page 33
- Configuring the RADIUS Attributes for SSG TCP Redirection, page 34
- Configuring Permanent TCP Redirection for HTTP Proxy Support, page 35
- Verifying SSG TCP Redirect for Services, page 37
- Troubleshooting SSG TCP Redirection, page 39

For conceptual information about SSG TCP Redirection features, see SSG TCP Redirect Features Overview, page 6.

Enabling SSG TCP Redirect for Services (Required)

To enable the SSG TCP Redirect for Services feature, use the following commands:

Note You must enable Cisco Express Forwarding (CEF) on the router before SSG functionality can be enabled.

SSG and Cisco Express Forwarding

SSG works with CEF switching technology to provide maximum Layer 3 switching performance. Because CEF is topology-driven rather than traffic-driven, its performance is unaffected by network size or dynamics.

Note CEF must be enabled for SSG to work.

Restrictions for SSG TCP Redirect for Services

SSG TCP Redirect for Services feature 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 must not be changed.
- Once the servers in a group have been configured, the routes to those servers do not change. SSG TCP Redirect for Services does not work if packets from servers that require redirection 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ssg enable**
5. **ssg tcp-redirect**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip cef** **Example:** `Router(config)# ip cef`	Enables global IP CEF on the router.
Step 4	**ssg enable** **Example:** `Router(config)# ssg enable`	Enables SSG functionality.
Step 5	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.

Defining a Captive Portal Group

To define a group of one or more servers that make up the captive portal group, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **server-group** *group-name*
5. **server** *ip-address port*
6. (Optional) Repeat steps 3. to 5. for each captive portal group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.
Step 4	**server-group** *group-name* **Example:** `Router(config-ssg-redirect)# server-group capt_portgroup`	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode. *group-name*—Name of the captive portal group.
Step 5	**server** *ip-address port* **Example:** `Router(config-ssg-redirect-group)# server 10.2.2.2 24`	Adds a server to a captive portal group. • *ip-address*—IP address of the server to add to the captive portal group. • *port*—TCP port of the server to add to the captive portal group.
Step 6	(Optional) Repeat steps 3. to 5. for each captive portal group.	Defines additional groups of servers to add to the captive portal group.

Configuring Initial and Periodic Captivation

To select the default captive portal group for initial captivation of users when they log in, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **redirect captivate initial default group** *group-name* **duration** *seconds*
5. **redirect captivate advertising default group** *group-name* **duration** *seconds* **frequency** *frequency*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.
Step 4	**redirect captivate initial default group** *group-name* **duration** *seconds* **Example:** `Router(config-ssg-redirect)# redirect captivate initial default group group-name duration seconds`	Selects the default captive portal group for initial captivation of users upon initialization. • *group-name*—Name of the captive portal group. • *seconds*—The duration in seconds of the initial captivation. The valid range is 1 to 65,536 seconds.
Step 5	**redirect captivate advertising default group** *group-name* **duration** *seconds* **frequency** *frequency* **Example:** `Router(config-ssg-redirect)# redirect captivate advertising default group group-name duration seconds frequency frequency`	Selects the default captive portal group for captivation of advertisements for users. • *group-name*—Name of the captive portal group. • *seconds*—The duration in seconds of the advertising captivation. The valid range is 1 to 65,536 seconds. • *frequency*—The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is 1 to 65536 seconds.

Associating an Access Control List with a Redirection Group

To associate an access control list with an SSG TCP redirection group, use the following commands:

Prerequisites

This task assumes that you know how to configure an IP access control list.

SUMMARY STEPS

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

   or

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect functionality and enters SSG-redirect configuration mode.
Step 4	**server-group** *group-name* **Example:** `Router(config-ssg-redirect)# server-group SESM1`	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode. • *group-name*—Name of the captive portal group.
Step 5	**server** *ip-address port* **Example:** `Router(config-ssg-redirect-group)# server 10.10.10.10 8080`	Adds a server to a captive portal group. • *ip-address*—IP address of the server to add to the captive portal group. • *port*—TCP port of the server to add to the captive portal group.
Step 6	**exit** **Example:** `Router(config-ssg-redirect-group)# exit`	Exits SSG-redirect-group configuration mode.

	Command or Action	Purpose

Step 7	**redirect port** *port-number* **to** *group-name*
	
	or
	
	redirect port-list *port-listname* **to** *group-name*
	
	Example:
	`Router(config-ssg-redirect)# redirect port 80 to SESM1`
	
	or
	
	`Router(config-ssg-redirect)# redirect port-list portlist1 to SESM1`
		(Optional) Configures a TCP port or named TCP port list for SSG TCP redirection.
		• **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.
		• *port-number*—Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
		• *group-name*—Defines the name of the captive portal group to redirect packets that are marked for a destination port or named TCP port list.
		• *port-listname*—Specifies the name of the named TCP port list.

Step 8	**redirect access-list** {*number* | *name*} **to** *group-name* **Example:** `Router(config-ssg-redirect)# redirect access-list 80 to SESM1`	Configures an access control list for SSG TCP redirection. • If a server group is not specified, the access list is used for redirection to any server group that does not have an access list associated with it.

Verifying SSG TCP Redirect Access Control Lists

Perform this task to verify that an access control list is associated with an SSG TCP redirection group.

SUMMARY STEPS

1. **show ssg tcp-redirect group**
2. **show ssg tcp-redirect group** *group-name*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show ssg tcp-redirect group**
	
	Example:
	`Router# show ssg tcp-redirect group`
	
	`Current TCP redirect groups:`
	`  SESM1`
	`  SESM2`
	`Default access-list: 101`
	`Default unauthenticated user redirect group: None Set`
	`Default service redirect group: None Set`
	`Prepaid user default redirect group: None Set`
	`SMTP forwarding group: None Set`
	`Default initial captivation group: None Set`
	`Default advertising captivation group: None Set`
		Displays a list of all defined portal groups.
		
		Verifies that the default access list for redirection is listed in the output.

Step 2	**show ssg tcp-redirect group** *group-name*
	
	Example:
	`Router# show ssg tcp-redirect group SESM1`
	
	`TCP redirect group SESM1:`
	`Showing all TCP servers (Address, Port):`
	`  10.1.1.1, 100,`
	`No redirectable destination networks defined.`
	`No redirectable TCP ports defined.`
	`Access list to match: 105`
		Displays a list of all defined portal groups for a server group with an access control list.
		
		Verifies that the redirected access control list is listed in the server group configuration in the output.

Configuring TCP Redirection of Unauthenticated Subscribers

To select a captive portal group for redirection of traffic from unauthorized users, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **redirect unauthenticated-user to** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.
Step 4	**redirect unauthenticated-user to** *group-name* **Example:** `Router(config-ssg-redirect)# redirect unauthenticated-user to mygroupname`	Selects a captive portal group for redirection of traffic from unauthenticated users. • *group-name*—Name of the captive portal group.

Configuring TCP Ports for Redirection

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **port-list** *port-listname*
5. **port** *port-number*
6. **exit**
7. **redirect port** *port-number* **to** *group-name*
   or
   redirect port-list *port-listname* **to** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.
Step 4	**port-list** *port-listname* **Example:** `Router(config-ssg-redirect)# port-list myportlist`	Defines the port list and enters SSG-redirect-port configuration mode. • *port-listname*—Defines the name of the port list.
Step 5	**port** *port-number* **Example:** `Router(config-ssg-redirect-port)# port 65534`	Adds a port to a port list. • *port-number*—Incoming destination port number. The valid range of port numbers is 1 to 65535
Step 6	**exit** **Example:** `Router(config-ssg-redirect-port)# exit`	Exits SSG-redirect-port configuration mode.

Step 7	**redirect port** *port-number* **to** *group-name*
	
	or
	
	redirect port-list *port-listname* **to** *group-name*
	
	Example:
	`Router(config-ssg-redirect)# redirect port 65534 to myportgroup`
	
	or
	
	`Router(config-ssg-redirect)# redirect port-list myportlist to myportgroup`
		Configures a TCP port or named TCP port list for SSG TCP redirection.
		• **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.
		• *port-number*—Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
		• *group-name*—Defines the name of the captive portal group to redirect packets that are marked for a destination port or named TCP port list.
		• *port-listname*—Specifies the name of the named TCP port list.

Configuring Unauthorized Service Redirection

To configure a destination network for unauthorized service redirection, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **network-list** *network-listname*
5. **network** *ip-address*
6. **exit**
7. **redirect unauthorized-service** [**destination network-list** *network-listname*] **to** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.
Step 4	**network-list** *network-listname* **Example:** `Router(config-ssg-redirect)# network-list mynetworklist`	Defines the network list and enters SSG-redirect-network configuration mode. • *network-listname*—Defines the name of the network list.
Step 5	**network** *ip-address* **Example:** `Router(config-ssg-redirect-network)# network ip-address 10.2.2.2`	Adds the specified IP address to the named network list. • *ip-address*—The IP address to add to a named network list.
Step 6	**exit** **Example:** `Router(config-ssg-redirect-network)# exit`	Exits SSG-redirect-network configuration mode.

	Command or Action	Purpose
Step 7	**redirect unauthorized-service** [**destination network-list** *network-listname*] **to** *group-name* **Example:** `Router(config-ssg-redirect)# redirect unauthorized-service destination network-list mynetworklist to myportgroup`	Creates a list of destination IP networks that can be redirected by the named captive portal group. • (Optional) **destination network-list—**Checks to determine if incoming packets from authenticated hosts require redirection to authorized networks. • (Optional) *network-listname*—Name of the list of destination IP networks. • *group-name*—Name of the captive portal group. **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 *group-name* argument is used as the default group for unauthorized service redirection when the IP address of the unauthorized packet does not fall into any network list associated with the captive portal group.

Configuring SMTP Redirection

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg tcp-redirect**
4. **redirect smtp group** *group-name* [**all** | **user**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg tcp-redirect** **Example:** `Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.
Step 4	**redirect smtp group** *group-name* [**all** | **user**] **Example:** `Router(config-ssg-redirect)# redirect smtp group myportgroup all`	Selects a captive portal group for redirection of SMTP traffic. • *group-name*—Name of the captive portal group. • (Optional) **all**—All SMTP packets are forwarded. • (Optional) **user**—Forwards SMTP packets from users who have SMTP forwarding permissions. **Note** If you do not configure the optional **all** or **user** keywords, the default is **all**.

Configuring the RADIUS Attributes for SSG TCP Redirection

To configure the RADIUS attributes for SSG TCP Redirection, use the vendor-specific 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 6 lists vendor-specific RADIUS attributes required in the user profile to perform SSG TCP redirection.

Table 6 Vendor-Specific RADIUS Attributes 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.

Configuring Permanent TCP Redirection for HTTP Proxy Support

To configure permanent TCP redirection for authenticated and unauthenticated users with HTTP proxy server configurations, perform this task.

Prerequisites for Configuring SSG Permanent TCP Redirection

Before configuring permanent TCP redirection, perform the following tasks:

- Configure captive portal server groups for authenticated and unauthenticated HTTP-proxy users, see "Defining a Captive Portal Group" section on page 24.
- Configure SESM to support SSG redirection.

Note To enable HTTP proxy users to reach SESM, provide a globally routable IP address to SESM.

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, see "RADIUS Attributes for SSG Permanent TCP Redirection" section on page 12.

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ssg tcp-redirect`
	
	Example:
	`Router(config)# ssg tcp-redirect`
		Enables SSG TCP redirect and enters SSG-redirect configuration mode.

	Command or Action	Purpose
Step 4	**redirect permanent http authenticated to** *server-group* **Example:** `Router(config-ssg-redirect)# redirect permanent http authenticated to auth_servergroup`	Specifies a server group for permanent TCP redirections for authenticated users with HTTP proxy server configurations. • *server-group*—Name of the local HTTP proxy server group for authenticated users
Step 5	**redirect permanent http unauthenticated to** *server-group* **Example:** `Router(config-ssg-redirect)# redirect permanent http unauthenticated to unauth_servergroup`	Specifies a server group for permanent TCP redirections for unauthenticated users with HTTP proxy server configurations. • *server-group*—Name of the local HTTP proxy server group for unauthenticated users
Step 6	**end** **Example:** `Router(config-ssg-redirect)# end`	(Optional) Returns to global configuration mode.
Step 7	Configure the RADIUS service profile to support permanent TCP redirection.	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: • ssg-service-info = KW*server-group-name* • ssg-service-info = KW0 See the "RADIUS Attributes for SSG Permanent TCP Redirection" section on page 12 for more information about the RADIUS attributes for permanent TCP redirection.

Verifying SSG TCP Redirect for Services

Use the following show commands to verify the SSG TCP Redirect for Services configuration.

SUMMARY STEPS

1. **show running-config**
2. **show ssg tcp-redirect group** [*group-name*]
3. **show ssg tcp-redirect mappings** [*ip-address* [*interface*]]
4. **show ssg host ip-address**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show running-config**
	
	Example:
	
	`Router# show running-config`
	
	`ssg tcp-redirect`
	` network-list RedirectNw`
	`  network 10.16.10.0 255.255.255.0`
	`  network 10.20.0.0 255.255.0.0`
	`!`
	`port-list WebPorts`
	` port 80`
	`.`
	`.`
	`.`
	`.`
		Displays the current SSG TCP Redirect for Services configuration.

Step 2	**show ssg tcp-redirect group** [*group-name*]
	
	Example:
	
	`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`
		Displays a list all configured captive portal groups, and indicates which group is used for redirected packets from unauthorized users.
		
		This show command also displays which captive portal groups are the default groups for captivation and unauthorized service redirection.
		
		• *group-name*—(optional) Name of the captive portal group.
		
		If you do not enter the optional *group-name* argument, the **show ssg tcp-redirect group** command displays a list of all defined portal groups. If the *group-name* argument is included, the command displays information about the specified portal group.

Command or Action	Purpose

Step 3 **show tcp-redirect mappings** [*ip-address* [*interface*]]
 	
Example:
 	
`Router# show tcp-redirect mappings`
 	
`Authenticated hosts:`
` TCP remapping Host:10.16.10.0 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:10.0.0.2 to server:10.2.36.253 on port:80 80`
 	
`Router# show tcp-redirect mappings 10.16.0.0`
 	
`TCP remapping Host:10.16.10.0`
`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`
	Displays any direct mappings, and TCP redirect statements in the output.
	
	• *ip-address*—(optional) The host IP address.
	
	If you do not enter the optional *ip-address* argument, the **show tcp-redirect mappings** command displays a list of IP addresses for all hosts with stored mappings. If the *ip-address* argument is included, all mappings for the host with the specified IP address are displayed.
	
	• *interface*—(optional) The interface on which the host is connected to SSG.
	
	Use the optional *interface* argument 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.

	Command or Action	Purpose

Step 4	**show ssg host** *ip-address*
	
	Example:
	
	`Router# show ssg host 10.16.0.0`
	
	`--------- HostObject Content --------------`
	`Activated:TRUE`
	`Interface:`
	`User Name:dev-user1`
	`Host IP:10.16.0.0`
	`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; tunnel1; proxy1; passthru1;`
	`Subscribed Service Groups:NONE`
		Displays information about a subscriber that is specified by the entered IP address.

Troubleshooting SSG TCP Redirection

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

SUMMARY STEPS

1. **show ssg host** [*ip-address*]
2. **show ssg tcp-redirect group** [*group-name*]
3. **show tcp-redirect mappings** [*ip-address*] [*interface*]
4. **debug ssg tcp-redirect** {**packet** | **error** | **event**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ssg host** [*ip-address*] **Example:** `Router# show ssg host 10.168.0.0`	Displays information about a subscriber and current connections of the subscriber.
Step 2	**show ssg tcp-redirect group** [*group-name*] **Example:** `Router# show ssg tcp-redirect group mygroup`	Lists all configured captive portal groups and indicates which group receives redirected packets from unauthorized users. If the *group-name* is specified, this command displays detailed information about that captive portal group.
Step 3	**show tcp-redirect mappings** [*ip-address*] [*interface*] **Example:** `Router# show tcp-redirect mappings 10.168.0.1 myinterface`	Displays the redirect mappings currently stored in SSG. If the host *ip-address* 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.
Step 4	**debug ssg tcp-redirect** {**packet** | **error** | **event**} **Example:** `Router# debug ssg tcp-redirect packet`	Use this command to turn on debug information for the SSG TCP Redirect for Services feature. • **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. **Note** This command replaces the **debug ssg http-redirect** command.

Configuring a Per-Session Firewall

SSG uses Cisco IOS software access control lists (ACLs) to prevent users, services, and pass-through traffic from accessing specific IP addresses and ports. This is known as a per-session firewall.

Note Certain restrictions apply when configuring per-session firewalls. Before configuring a per-session firewall, see Per-Session Firewall Overview, page 13.

To configure SSG ACLs, configure the following Cisco-AV pair attributes in your user or service profile on the AAA server:

- Downstream Access Control List (outacl)

  Cisco-AVpair = "ip:outacl[**#***number*]**=**{*standard-access-control-list* | *extended-access-control-list*}**"**

- Upstream Access Control List (inacl)

  Cisco-AVpair = "ip:inacl[**#***number*]**=**{*standard-access-control-list* | *extended-access-control-list*}"

Note The method used to configure these attributes depends upon the AAA server. see your AAA server documentation for details.

Example Configuration for Per-Session Firewall

The following is an example of a downstream ACL (outacl):

```
Cisco-AVpair = "ip:outacl#101=deny tcp 10.168.1.0 0.0.0.255 any eq 21"
```

The following is an example of an upstream ACL (inacl):

```
Cisco-AVpair = "ip:inacl#101=deny tcp 10.168.1.0 0.0.0.255 any eq 21"
```

Configuring Default DNS Redirection

Note Certain restrictions apply when configuring default DNS redirection. Before configuring default DNS redirection, see Default DNS Redirection Overview, page 15.

Perform the following tasks to configure default DNS redirection:

- Configuring DNS Redirection in a Local Service Profile using the Cisco IOS CLI, page 41
- Configuring Dynamic DNS Assignment on the AAA Server, page 42
- Configuring DNS Fault tolerance, page 43

For conceptual information about default DNS redirection, see Default DNS Redirection Overview, page 15.

Configuring DNS Redirection in a Local Service Profile using the Cisco IOS CLI

This task configures SSG default DNS redirection in a local service profile.

You can also configure SSG default DNS redirection by adding the VSA for default DNS redirection to the service profile on the RADIUS server. See the SSG Domain Name Vendor-Specific Attribute, page 16 for information about the Domain Name VSA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **local-profile** *profile-name*
4. **attribute 26 9 251 "O*[;unauthenticated]"**
5. **end**
6. **show ssg service** [*service-name* [**begin** *expression* | **exclude** *expression* | **include** *expression*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**local-profile** *profile-name* **Example:** `Router(config)# local-profile og-dns`	Configures a local service profile and enters profile configuration mode.
Step 4	**attribute 26 9 251 "O*[;unauthenticated]"** **Example:** `Router(config-prof)# attribute 26 9 251 "O*"`	Configures the attribute for default DNS redirection in a local service profile.
Step 5	**end** **Example:** `Router(config-prof)# end`	(Optional) Returns to privileged EXEC mode.
Step 6	**show ssg service** [*service-name* [**begin** *expression* | **exclude** *expression* | **include** *expression*]] **Example:** `Router# show ssg service og-dns`	(Optional) Displays the information for about a service. The output for this command indicates if default DNS matching is enabled and whether it is valid for unauthenticated users only.

Configuring Dynamic DNS Assignment on the AAA Server

This feature works automatically and is dependent on what SSG receives from a remote AAA server. No configuration is required on the SSG itself. These attributes must be configured in the relevant "service profile" on the AAA server.

For proxy services, the DNS address(es) are signaled in the Access-Accept from the proxy AAA server. This can be via one of the following attributes:

- Cisco AV-pairs ("ip:dns-servers=10.44.216.10 171.69.11.48")
- Ascend Non-Standard attributes (attrs#135 and #136)

SSG recognizes DNS addresses that are communicated in either of these formats and associates them with the relevant service and connection using the previously stated algorithm.

For details of the Cisco AV attributes see Restrictions for Dynamic DNS Assignment, page 17.

Configuring DNS Fault tolerance

You can also configure SSG default DNS tolerance by adding the VSA for default DNS redirection to the service profile on the RADIUS server.

See the SSG Domain Name Vendor-Specific Attribute, page 16 for information about the Domain Name VSA.

Configuration Examples for Configuring SSG Subscriber Experience Features

This section provides the following configuration examples:

- Enabling SSG TCP Redirect for Services: Example, page 43
- Defining a Captive Portal Group: Example, page 43
- Excluding Specific Traffic from Redirection: Example, page 44
- Redirecting Traffic from Unauthenticated Users: Example, page 44
- Configuring TCP Redirection of Unauthenticated Subscribers: Example, page 44
- TCP Ports for a Portal Group Configuration: Example, page 44
- Default Portal Group for Captivation: Example, page 45
- Destination Networks Configuration: Example, page 45
- Portal Group for SMTP Redirect Configuration: Example, page 46
- RADIUS Attributes for SSG TCP Redirect Configuration: Example, page 46
- SSG Default DNS Redirection Configuration: Example, page 47
- SSG Default DNS Redirection for Unauthenticated Users Configuration: Example, page 47

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 10.16.0.0 and port 8080, and the server with IP address 10.32.10.0 and port 8081, are added to the captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
 server-group RedirectServer
 server 10.16.0.0 8080
 server 10.32.10.0 8081
```

Excluding Specific Traffic from Redirection: Example

The following example shows how to redirect packets that are not destined to server 10.0.0.1 for initial captivation:

```
ssg tcp-redirect
 server-group InitialCapt
  server 10.1.1.1 8090
 !
 redirect port 80 to InitialCapt
 redirect access-list 101 to InitialCapt
 !
 redirect captivate initial default group InitialCapt duration 30
!
access-list 101 deny   ip any host 10.0.0.1
access-list 101 permit ip any any
```

Redirecting Traffic from Unauthenticated Users: Example

The following example shows how to redirect unauthenticated host traffic from subnet 10.1.0.0/16 to server group SESM1. Any other unauthenticated host traffic is redirected to SESM2.

```
ssg tcp-redirect
 server-group SESM1
  server 10.2.36.253 8080
 !
 redirect port 80 to SESM1
 redirect access-list 50 to SESM1
 redirect unauthenticated user to SESM1
 !
 server-group SESM2
  server 10.2.36.254 8080
 !
 redirect port 80 to SESM2
 redirect unauthenticated user to SESM2
 redirect access-list 101
 !
access-list 50 permit 10.1.0.0 0.0.255.255
```

Configuring TCP Redirection of Unauthenticated Subscribers: 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
```

TCP Ports for a Portal Group Configuration: Example

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
```

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 login) 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 the 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
```

Destination Networks Configuration: Example

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 10.16.10.0 255.255.255.0 and 10.20.0.0 255.255.255.0 are added to the network list named "RedirectNw."

```
ssg enable
ssg tcp-redirect
 network-list RedirectNw
  network 10.16.10.0 255.255.255.0
  network 10.20.0.0 255.255.255.0
 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 10.16.10.0 255.255.255.0
  network 10.20.0.0 255.255.255.0
```

```
exit
redirect unauthorized-service to RedirectServer
```

Portal Group for SMTP Redirect Configuration: Example

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
```

RADIUS Attributes for SSG TCP Redirect Configuration: Example

Note The RADIUS attributes shown in the following examples 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 login to one of the servers in the captive portal group named "CaptivateGrpA" for 300 seconds:

```
ICaptivateGrpA;300
```

The following example shows how to configure the user profile for initial captivation upon service login to the service "Games":

```
ICaptivateGrpB;240;Games
```

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

```
ACaptivateGrpA;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 "CaptivateGrpB" for 240 seconds. The captivation of advertisements begins when the user starts using the "Games" service and approximately every 1800 seconds thereafter:

```
ACaptivateGrpB;240;1800;Games
```

SSG Default DNS Redirection Configuration: Example

In the following example, all DNS packets are directed to the DNS server 10.6.6.2.

```
! Define the service profile locally
local-profile og-dns
 attribute 26 9 251 "D10.6.6.2"
 attribute 26 9 251 "R10.6.6.2;255.255.255.255"
 attribute 26 9 251 "O*"
!
! Make the service an open garden
ssg open-garden og-dns
```

When a default DNS domain is configured, the output for the **show ssg service** command includes the following:

```
Default domain matching is Enabled
```

SSG Default DNS Redirection for Unauthenticated Users Configuration: Example

The following example shows how default DNS matching is applied only to unauthenticated users. If the user is authenticated, the packet is processed normally.

```
! Define the service profile locally
local-profile og-dns-non-authen
 attribute 26 9 251 "D10.6.6.2"
 attribute 26 9 251 "R10.6.6.2;255.255.255.255"
 attribute 26 9 251 "O*;unauthenticated"
!
! Make the service an open garden
ssg open-garden og-dns-non-authen
```

When a default DNS domain is configured for unauthenticated users only, the output for the **show ssg service** command includes the following:

```
Default domain matching is Enabled - valid only for unauthenticated users
```

Additional References

The following sections provide references related to SSG subscriber experience features.

Related Documents

Related Topic	Document Title
Configuring SESM	*Cisco Subscriber Edge Services Manager* documentation
RADIUS commands	*Cisco IOS Security Command Reference*
RADIUS configuration tasks	"Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*
SSG commands	*Cisco IOS Service Selection Gateway Command Reference*

Standards

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

MIBs

MIB	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

RFC	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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring SSG Subscriber Experience Features

Table 7 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the *Service Selection Gateway Features Roadmap*.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 7 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 7 Feature Information for Configuring SSG Subscriber Experience Features

Feature Name	Releases	Feature Configuration Information
Hierarchical Policing	12.2(4)B 12.2(13)T	The SSG Hierarchical Policing feature ensures that a subscriber does not utilize additional bandwidth for overall service or for a specific service that is outside the bounds of the subscriber's contract with the service provider. The following section provides information about this feature: • "SSG Hierarchical Policing Overview" on page 3 • "Configuring SSG Hierarchical Policing" on page 18 • "Configuration Examples for Configuring SSG Subscriber Experience Features" on page 43
SSG TCP Redirect	12.1(5)DC 12.2(4)B 12.2(8)T 12.3T 12.4	The SSG TCP Redirect feature redirects certain packets, which would otherwise be dropped, to captive portals that can handle the packets in a suitable manner. The following sections provide information about this feature: • "SSG TCP Redirect Features Overview" on page 6 • "Configuring SSG TCP Redirection Features" on page 22 • "Configuration Examples for Configuring SSG Subscriber Experience Features" on page 43 The following commands are introduced in this feature: **ssg tcp-redirect**, **redirect unauthenticated-user to**.

Table 7 Feature Information for Configuring SSG Subscriber Experience Features (continued)

Feature Name	Releases	Feature Configuration Information
Per-Session Firewall	12.0(3)DC 12.2(4)B 12.2(8)T	The SSG Per Session Firewall feature enables you to configure Cisco IOS software access control lists (ACLs) to prevent users, services, and pass-through traffic from accessing specific IP addresses and ports. The following section provides information about this feature: • "Per-Session Firewall Overview" on page 13 • "Configuring a Per-Session Firewall" on page 40 • "Configuration Examples for Configuring SSG Subscriber Experience Features" on page 43
DNS Redirection	12.3(3)B 12.3(7)T	The SSG DNS Redirection feature enables you to match a domain name server (DNS) request to the appropriate domain name service, based on attributes of the user requesting the service. When the Cisco SSG receives a Domain Name System (DNS) request, it performs domain-name matching by using the domain-name attribute from the service profiles of the currently logged-in services. If a match is found, the request is redirected to the DNS server for the matched service. If a match is not found and the user is logged in to a service that has Internet connectivity, the request is redirected to the first service in the user's service access order list that has Internet connectivity. If a match is not found and the user is not logged in to a service that has Internet connectivity, the request is forwarded to the DNS server defined in the client's TCP/IP stack. The following section provides information about this feature: • "Default DNS Redirection Overview" on page 15 • "Configuring Default DNS Redirection" on page 41 • "Configuration Examples for Configuring SSG Subscriber Experience Features" on page 43
Configuring SSG Subscriber Experience Features	15.0(1)M	This feature was removed in Cisco IOS Release 15.0(1)M.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.