SSG—Limiting the Number of Sessions and Services

This feature allows you to limit the number of user sessions and services allowed on a Service Selection Gateway (SSG) device. A Cisco device that is running a Cisco IOS image with SSG is referred to as an SSG.

You can set limits for:

- The number of host objects that can be activated on the SSG device
- The number of services available to each user
- The number of transparent auto logon (TAL) users on an SSG device

Setting any of these limits helps to ensure that the SSG device's resources are not exhausted during extreme network loads.

History for the SSG-Limiting the Number of Sessions and Services Feature

Release	Modification
Cisco IOS Release 12.4(2)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

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

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

Contents

This document includes the following topics:

Prerequisites

Before you can use this SSG feature to limit sessions and services, you must:

- Globally enable IP CEF before using SSG.
- Install and configure Cisco Subscriber Edge Services Manager (SESM) as described in the *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*.
- Enable Cisco Express Forwarding (CEF) on all logical and physical interfaces.
- Configure an Authentication, Authorization, and Accounting (AAA) RADIUS server or an LDAP server to authenticate subscribers and to store subscriber and service profiles.

Restrictions

The following restriction applies to this SSG feature:

- SSG does not process IP multicast packets. IP multicast packets are handled by Cisco IOS software.

Configuring SSG to Limit Sessions and Services

To configure this SSG feature to limit sessions and services, perform the following tasks:

Limit the Number of Host Objects on an SSG Device

This section describes how you can use the **ssg maximum host** command to limit the number of host objects that can be enabled on an SSG device. Using this command helps to prevent a router from experiencing resource exhaustion when the number of logon-requests exceed the router's limitations.

This section includes the following topics:

SUMMARY STEPS

This section lists the command sequence required to limit the number of host objects that can be enabled on an SSG device.

For a detailed summarization of the command sequence, with examples, refer to DETAILED STEPS, next.

1. **enable**
2. **configure terminal**
3. **ssg maximum host** *number-of-hosts*
4. **end**

DETAILED STEPS

This section provides a detailed summarization of the command sequence, with examples, required to limit the number of host objects that can be enabled on an SSG device.

	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 maximum host** *number-of-hosts* **Example:** `Router(config)# ssg maximum host 100`	Limits the number of hosts permitted on an SSG device. The valid range of hosts is 1 to 2147483647.
Step 4	**end** **Example:** `Router(config)# end`	Exits privileged EXEC mode.

What Happens When a Router Reaches the Maximum Number of Host Connections

After a router reaches the maximum number of allowable host connections, it does not accept any new connections. When it receives a new connection request, the router replies with an Access-Reject message, which indicates the router has reached the maximum number of allowable host connections (refer to Figure 1).

The method of informing users depends on the type of user login:

- If a user attempts to log in using the Subscriber Edge Services Manager (SESM) dashboard, he or she receives an Access-Reject message and an error code of 57 to indicate that the router has reached the maximum number of host connections.
- A user who attempts to log in using a RADIUS proxy, receives an Access-Reject message.
- A user who attempts to log in using PPP can have a session established, but the session is then brought down again.

Figure 1 Access-Reject message

```
SSG_MAX_HOST: SSG host count has reached the maximum configured value of xx.
The number of SSG hosts has reached the maximum configured limit. New hosts
will not be allowed to log in until some users log out.
```

Limit the Number of Transparent Autologon Users

The SSG Transparent Autologon (TAL) feature allows users with authorized IP addresses to “pass through” to an SSG device. Allowing an unlimited number of TAL users on an SSG device can cause resource exhaustion. To help preserve router resources, you can use the **user passthrough maximum** command to limit the number of TAL users.

This section includes the following topics:

SUMMARY STEPS

This section lists the command sequence required to limit the number of TAL users on an SSG device.

For a detailed summarization of the command sequence, with examples, refer to DETAILED STEPS, next.

1. **enable**
2. **configure terminal**
3. **ssg login transparent**
4. **user passthrough maximum** *number-of-users*
5. **end**
6. **end**
7. **end**

DETAILED STEPS

This section provides a detailed summarization of the command sequence, with examples, required to limit the number of TAL users on an SSG device.

	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 login transparent** **Example:** `Router(config)# ssg login transparent`	Enables SSG login transparent submode.
Step 4	**user passthrough maximum** *number-of-users* **Example:** `Router(config-login-transparent)# user passthrough maximum 100`	Limits the number of TAL users. The valid range of users is 1 to 2147483647.
Step 5	**end** **Example:** `Router(config-login-transparent)# end`	Exits TAL mode.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config)# end`	Exits global configuration mode.
Step 7	**end** **Example:** `Router# end`	Exits privileged EXEC mode.

What Happens When the Number of TAL Users Reaches the Specified Limit

When a router reaches the limit of TAL users, SSG does not allow transparent authorization of new IP addresses. All new users are marked as *unidentified*. The following error message is also displayed on the SSG router console (refer to Figure 2):

Figure 2 Max_TAL error message

```
SSG_TAL_TP_MAX: Transparent passthrough users count has reached the maximum
configured value. New transparent passthrough users will not be allowed to
login until some existing transparent passthrough users are cleared.
```

Limit the Number of User Services

You can use the **ssg maximum service** command to limit the number of services available to each user. Limiting the number of services available to each user, helps prevent a router from experiencing resource exhaustion.

Note The **ssg maximum service** command replaces the **ssg maxservice** command. You can still use the **ssg maxservice** command, but when you save the configuration, that command changes to the **ssg maximum service** command in the saved configuration.

This section includes the following topics:

SUMMARY STEPS

This section lists the command sequence required to limit the number of services available to each user on an SSG device.

For a detailed summarization of the command sequence, with examples, refer to DETAILED STEPS, next.

1. **enable**
2. **configure terminal**
3. **ssg maximum service** *number-of-services*
4. **end**

DETAILED STEPS

This section provides a detailed summarization of the command sequence, with examples, required to limit the number of services available to each user on an SSG device.

	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 maximum service** *number-of-services* **Example:** `Router(config)# ssg maximum service 5`	Limits the number of services available to each user on an SSG device. The valid range is 1 to 20.
Step 4	**end** **Example:** `Router(config)# end`	Exits privileged EXEC mode. Alternatively, you can press Ctrl-Z.

What Happens When Users Attempt to Exceed the Maximum Number of Services

When a user attempts to exceed the maximum number of services (as specified in the command), those services do not become available.

Configuration Example for SSG-Limiting the Number of Sessions and Services

In the following configuration example, all three feature options (**ssg maximum host**, **ssg maximum service**, and **user passthrough maximum**) are configured on an SSG device. In this configuration example, host objects and user services are limited to 10, and TAL users are limited to 100.

```
Router> enable
Router# configure terminal
Router(config)# ssg maximum host 10
Router(config)# ssg maximum service 10
Router(config)# ssg login transparent
Router(config-login-transparent)# user passthrough maximum 100
```

Additional References

The following sections provide references related to SSG-Limiting the Number of Sessions and Services.

Related Documents

Related Topic	Document Title
SSG commands	*Cisco IOS Service Selection Gateway Command Reference*, Release 12.4T
SSG configuration tasks	*Cisco IOS Service Selection Gateway Configuration Guide*, Release 12.4
SESM	Cisco *Subscriber Edge Services Manager* documentation
RADIUS commands	Cisco IOS Security Command Reference, Release 12.4T
RADIUS configuration tasks	*Cisco IOS Security Configuration Guide*, Release 12.4T

Standards

Standard	Title
IEEE 802.11b	*IEEE Wireless Standards*

MIBs

MIB	MIBs Link
The Service Selection Gateway MIB enables network administrators to use Simple Network Management Protocol (SNMP) to monitor and manage SSG. The SSG MIB contains objects that correspond to and allow the monitoring of several important SSG features. For a detailed list of MIB objects and their definitions, see the CISCO-SSG-MIB.	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
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*
RFC 2866	*RADIUS Accounting*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new commands only.

- **ssg maximum host**
- **ssg maximum service**
- **user passthrough maximum**

ssg maximum host

To limit the number of user connections (hosts) allowed on a Service Selection Gateway (SSG) device, use the **ssg maximum host** command in global configuration mode. To remove the limitation on the number of hosts, use the **no** form of this command.

ssg maximum host *number-of-hosts*

no ssg maximum host *number-of-hosts*

Syntax Description

number-of-hosts	Limits the number of host objects allowed on an SSG device. Range: 1 to 2147483647.

Command Default

Unlimited hosts are allowed on an SSG device.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command prevents resource exhaustion on a router by limiting the number of host connections. When the router reaches the maximum number of connections, it refuses any new connections. As users log out, new users are allowed to connect.

This command limits only the number of host connections; it does not limit the number of services available to users.

Examples

The following example limits the number of host connections to 1,000:

```
Router(config)# ssg maximum host 1000
```

Related Commands

Command	Description
ssg maximum service	Limits the number of services available to SSG users.
user passthrough maximum	Limits the number of SSG transparent autologon users on an SSG device.

ssg maximum service

To limit the number of services available to a user on a Service Selection Gateway (SSG) device, use the **ssg maximum service** command in global configuration mode. To remove the limitation on the number of services, use the **no** form of this command.

ssg maximum service *number-of-services*

no ssg maximum service *number-of-services*

Syntax Description

number-of-services	Limits the number of services available to a user on an SSG device. The valid range of services is 1 to 20.

Command Default

Users have up to 20 services available.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command enables you to limit the number of services available to a user. This command replaces the **ssg maxservice** command. If you issue the **ssg maxservice** command and save your configuration, the saved configuration shows the **ssg maximum service** command.

Examples

The following example limits the number of user services to 10:

```
Router(config)# ssg maximum service 10
```

Related Commands

Command	Description
ssg maximum host	Limits the number of host connections on an SSG device.

user passthrough maximum

To limit the number of Service Selection Gateway (SSG) transparent autologon (TAL) users on an SSG device, use the **user passthrough maximum** command in SSG login transparent submode. To remove the limitation on the number of SSG TAL users, use the **no** form of this command.

user passthrough maximum *number-of-users*

no user passthrough maximum *number-of-users*

Syntax Description

number-of-users	Limits the number of SSG TAL users on an SSG device. Range: 1 to 2147483647.

Command Default

Unlimited TAL users can access an SSG device.

Command Modes

SSG login transparent submode

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command prevents resource exhaustion on a router by limiting the number of SSG TAL users on a device. When the router reaches the maximum number of users, it refuses any new connections.

Examples

The following example limits the number of SSG TAL users to 400:

```
Router(config)# ssg logon transparent
Router(config-login-transparent)# user passthrough maximum 400
```

Related Commands

Command	Description
ssg maximum host	Limits the number of host connections on an SSG device.
ssg maximum service	Limits the number of services available to a user on an SSG device.