



Service Selection Gateway Hierarchical Policing

Feature History

Release	Modification
12.2(4)B	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.

This document describes the SSG AutoLogon Using Proxy Radius feature and contains the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 6](#)
- [Supported Standards, MIBs, and RFCs, page 6](#)
- [Configuration Tasks, page 7](#)
- [Monitoring and Maintaining SSG Hierarchical Policing, page 9](#)
- [Configuration Examples, page 9](#)
- [Command Reference, page 15](#)

Feature Overview

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

SSG allows subscribers to choose one or more types of services. Each type of service has its own bandwidth requirements; for instance, 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. SSG, therefore, requires a mechanism to ensure bandwidth is distributed properly for customers using different types of services.

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 all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-session policing to ensure 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 destined to or sent from a particular subscriber and can only police the bandwidth allocated to a subscriber. Per-user policing 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. Per-session policing is useful when an SSG subscriber is subscribed to more than one service and the multiple services are allocated different amounts of bandwidth; for instance, suppose a single subscriber is paying separately for Internet access and video service but is receiving both services from the same service provider. The video service would likely be allocated more bandwidth than the Internet access service and would likely cost more to the subscriber. Per-session policing 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.

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, time between packets and packet sizes, ultimately determine whether a packet is transmitted or dropped.

The following sections explain the aspects of the 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.

The token bucket algorithm used in SSG Hierarchical Policing 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.

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

Table 1 SSG Hierarchical Policing User-Configurable Parameters

Parameter	Purpose
committed-rate	<p>The committed rate is the amount of bandwidth that is entitled to a subscriber (per-user policing) or a service to a particular subscriber (per-session policing). The token bucket algorithm uses the committed rate parameter when generating tokens when a packet arrives.</p> <p>The committed rate should be equal to the minimum amount of bandwidth that is guaranteed to a subscriber or service. It is important to note that the committed rate is specified in bits per second, while the normal burst and excess burst sizes are specified in bytes.</p>
normal-burst	The normal burst parameter determines the maximum size of a traffic burst before packets are dropped.
excess-burst	<p>The excess burst size is an optional variable that determines the burst size beyond which all traffic is dropped. The excess burst size is used to support bursty traffic and is disabled when set lower than the normal burst size.</p> <p>If the excess burst size is configured, the traffic that falls between the normal burst 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.</p> <p>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 using the Random Early Detection [RED] feature).</p>

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.

If a user or a service has been idle for a long period of time, the likelihood that a larger packet is forwarded is increased.

The following table provides a definition of actual and compound debt:

Table 2 Actual and Compound Debt Definitions

Term	Definition
actual debt	<p>The actual debt is the number of tokens that have been borrowed by the current packet.</p> <p>When a packet is forwarded 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 using the excess burst (which is possible when the excess burst size is larger than the normal burst size).</p>
compound debt	<p>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.</p> <p>Compound debt is only a factor in forwarding a packet after the actual debt exceeds the normal burst size.</p> <p>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.</p>

Token Bucket Algorithm Calculations

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

-
- Step 1** The packet arrives. The packet size (Ps) is noted.
- Step 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).
- Step 3** The actual debt is calculated. The actual debt is calculated based on the following formula:
- $$\text{actual_debt} = \text{previous_actual_debt (Ad)} + \text{Ps}$$
- Step 4** The tokens that can be generated by the arriving packet are calculated:
- $$\text{tokens} = \text{committed_rate (Ar)} * \text{td}$$
- Step 5** The tokens are then compared to the actual debt.
- If $\text{tokens} > \text{actual_debt}$, the actual debt for the packet is set at 0.
 - If $\text{tokens} < \text{actual_debt}$, the actual debt is calculated using the following formula:
- $$\text{actual_debt} = \text{actual_debt} - \text{tokens}$$
- Step 6** The actual debt is compared to the normal burst to see if traffic should be forwarded or dropped.
- If $\text{actual_debt} < \text{normal_burst}$, the packet conforms and is forwarded.
 - If $\text{actual_debt} > \text{normal_burst}$, the packet is dropped if the excess burst size is not configured. If $\text{actual_debt} > \text{normal_burst}$ and the excess burst size is configured, compound debt is checked.

- c. The compound debt is calculated using the following formula:
$$\text{compound_debt} = \text{previous_compound_debt} + (\text{actual_debt} - \text{normal_burst})$$
- d. If $\text{compound_debt} < \text{excess_burst}$, the packet is forwarded.
- e. If $\text{compound_debt} > \text{excess_burst}$, the packet is dropped.

Benefits

Guarantees Fairness Among Bandwidth Allocated to SSG Subscribers and Services

The SSG Hierarchical Policing feature helps ensure 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.

Restrictions

- This feature only works in the Cisco Express Forwarding (CEF) switching path.
- The committed rate parameter must be configured at 8000 or larger. If the committed rate is set lower than 8000, it will automatically be configured at 8000.
- If the committed rate parameter is set between 8000 and 16000, the parameter values will be altered based on the following formula:
$$(\text{committed_rate} * 16) / 8000$$
- If the normal burst parameter is less than the IP maximum transmission unit (MTU) of an interface, the normal burst parameter will be set equal to the IP MTU of the interface.
- Only packets destined to subscribed services will be policed. The following packets cannot be policed using this feature:
 - Domain Name System (DNS) packets
 - Multicast packets
 - Open garden packets
 - Default network packets

Related Features and Technologies

- Service Selection Gateway (SSG)
- Authorization, Authentication, and Accounting (AAA)

Related Documents

- *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

- Cisco 6400 series routers
- Cisco 7200 series routers
- Cisco 7401ASR routers

Availability of Cisco IOS Software Images

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

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

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

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

RFCs

None

Configuration Tasks

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

- [Configuring RADIUS User and Service Profiles for SSG Hierarchical Policing](#) (required)
- [Enabling SSG Hierarchical Policing](#) (required)
- [Verifying SSG Hierarchical Policing](#) (optional)

Configuring RADIUS User and Service Profiles for SSG Hierarchical Policing

User profiles and service profiles in RADIUS need to be modified in order to enable SSG Hierarchical Policing.

For per-user policing, the RADIUS user profile of the subscriber has to be modified to accommodate SSG Hierarchical Policing.

For per-session policing, the RADIUS service profile (which can be configured in a remote AAA server or locally) has to be modified to accommodate SSG Hierarchical Policing.

Configuring a RADIUS Profile for Per-User Policing

The SSG subscriber being policed has to have the proper RADIUS user profile in order to enable per-user policing:

Account-Info = “**QU**;upstream-token-rate;upstream-normal-burst;
[upstream-excess-burst];**D**;downstream-token-rate;
downstream-normal-burst;[downstream-excess-burst]”

Configuring SSG Hierarchical Policing Parameters in a RADIUS Service Profile

For per-session policing, the RADIUS service profile (which can be configured in a remote AAA server or locally) has to be modified to accommodate SSG Hierarchical Policing.

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

	Command	Purpose
Step 1	Router(config)# local-profile <i>profile-name</i>	Enters profile configuration mode. Configures a local RADIUS service profile.
Step 2	Router(config-prof)# attribute <i>radius-attribute-id</i> <i>vendor-id cisco-vsa-type</i> "QU;upstream-token-rate;upstream-normal-burst; [upstream-excess-burst];D;downstream-token-rate; downstream-normal-burst;downstream-excess-burst"	Configures the policing attributes in a local RADIUS service profile. The Q parameter is used to represent 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.

To configure a service profile on the AAA server, use the following service profile attribute:

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

Enabling SSG Hierarchical Policing

After the parameters for SSG Hierarchical Policing are configured in the user or service profile, the **ssg qos police** command must be entered on the router to enable per-user or per-session policing.

To enable SSG per-user policing on the router, enter the following command:

Command	Purpose
Router(config)# ssg qos police user	Enables SSG per-user policing.

To enable SSG per-session policing, enter the following command:

Command	Purpose
Router(config)# ssg qos police session	Enables SSG per-session policing.

The **no** forms of these commands, **no ssg qos police user** and **no ssg qos police session**, can be used to disable SSG Hierarchical Policing on a router.

Verifying SSG Hierarchical Policing

The following commands can be entered to verify the SSG Hierarchical Policing feature:

Command	Purpose
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. The show ssg host command should be used to verify per-user policing.
Router# show ssg connection	Displays information about a particular SSG connection, including the policing parameters.

Monitoring and Maintaining SSG Hierarchical Policing

Command	Purpose
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. The show ssg host command should be used to verify per-user policing.
Router# show ssg connection	Displays information about a particular SSG connection, including the policing parameters.
Router# debug ssg data	Displays SSG QoS information.

Configuration Examples

This section provides the following configuration examples:

- [Per-User Policing without Excess Burst Example](#)
- [Per-User Policing with Excess Burst Example](#)
- [Per-Session Policing Example](#)
- [Verifying a Policing Configuration Example](#)

Per-User Policing without Excess Burst Example

This section provides an example of a per-user policing configuration. This example provides configuration pointers and also demonstrates how theoretical traffic would be policed according to this configuration.

The following is an example of a user profile with the SSG Hierarchical Policing enabled for downstream traffic. In this example, an excess burst size is set at 0 so all dropped packets are tail-dropped. In this particular profile, only downstream traffic is policed (although it is important to note that an upstream token bucket algorithm would operate identically to the downstream policing algorithm).

```
user = johndoe
radius = 7200-SSG-v1.1
check_items= {
2 = cisco
}
reply_attributes={
9,250="Nproxy_ser"
9,250="Ntunnel_ser"
9,250="QD8000;2000;0"
```

Per-user policing must be enabled on the router before the traffic directed to the subscriber is policed. Per-user policing is enabled on the router by entering the following global configuration command:

```
Router(config)# ssg qos police user
```

The following steps provide an example of how traffic going to the subscriber is treated based on the above configuration. Because packet sizes are variable, the packet sizes used in this example are created for the sake of the example.

The token bucket starts at 1000 tokens; remember that the committed rate is specified in bits per seconds, but that the token bucket operates based on bytes. Hence, 8000 bits is equal to 1000 bytes, so a full token bucket has 1000 tokens. The normal burst parameter is set at 2000. For the sake of the example, no actual debt has been accrued before the arrival of the first packet.

- The first packet is 500 bytes and arrives 3/4 of a second after the last packet.
 - The packet size is 500 bytes.
 - The time difference (td) is 3/4 of a second.
 - $\text{actual_debt} = \text{previous_actual_debt} + \text{packet_size} = 0 + 500 = 500$
 - $\text{tokens} = \text{committed_rate} * \text{td} = 1000 * 3/4 = 750$
 - $750 > 500$. Therefore, the tokens are greater than the actual debt.

Because tokens are greater than the actual debt, the user has been idle for a sufficient amount of time and the packet is transmitted.
- The second packet is 1500 bytes and arrives 1/2 a second after the previous packet.
 - The packet size is 1500 bytes.
 - The td is 1/2 of a second.
 - $\text{actual_debt} = 0 + 1500 = 1500$
 - $\text{tokens} = 1000 * 1/2 = 500$
 - $500 < 1500$. Therefore, the tokens are less than the actual debt. Because the tokens are less than the actual debt, an updated actual debt needs to be calculated and compared to the normal burst size.
 - $\text{New actual_debt} = \text{previous_actual_debt} - \text{tokens} = 1500 - 500 = 1000$
 - Normal burst is configured at 2000.
 - $1000 < 2000$. Because the actual debt is less than the normal burst size, the packet is forwarded.

- The next packet is 4000 bytes and it arrives 1/2 a second later.
 - The packet size is 4000 bytes.
 - The td is 1/2 of a second.
 - $actual_debt = previous_actual_debt + packet_size = 1000 + 4000 = 5000$
 - $tokens = 1000 * 1/2 = 500$
 - $500 < 5000$. The tokens are less than the actual debt, so the new actual debt needs to be computed.
 - $actual_debt = previous_actual_debt - tokens = 5000 - 500 = 4500$
 - $4500 > 2000$. Because the actual debt is greater than the normal burst size, the packet is dropped.

Future packets will be policed similarly based on this algorithm.

Per-User Policing with Excess Burst Example

This section provides an example of a per-user policing configuration. This example provides configuration pointers and also demonstrates how theoretical traffic would be policed according to this configuration.

The following is an example of a user profile with the SSG Hierarchical Policing parameter configured. In this example, an excess burst size is specified. In this particular profile, only downstream traffic is policed (although it is important to note that an upstream token bucket algorithm would operate identically to the downstream policing algorithm). This user profile is formatted for use with a freeware RADIUS server:

```
bert Password = "ernie"  
  Session-Timeout = 21600,  
  Account-Info = "QD;16000;3000;4000"
```

In this user profile, the committed rate is set at 16000 bits per second (which is equal to 2000 bytes). The normal burst size is set at 3000 bytes and the excess burst size is set at 4000 bytes.

Per-user policing must be enabled on the router before the traffic directed to the subscriber is policed. Per-user policing is enabled on the router by entering the following command in global configuration mode:

```
Router(config)# ssg qos police user
```

The following steps provide an example of how traffic going to the subscriber is treated based on the above configuration. Because packet sizes are variable and unpredictable, the packet sizes used in this example are hypothetical.

- The first packet in this example is 1500 bytes and arrives when no debt has been accumulated by previous packets. Assume 1 second has passed since the last packet was transmitted.
 - The packet size is 1500.
 - The td is 1 second.
 - $\text{actual_debt} = \text{previous_actual_debt} + \text{packet_size} = 0 + 1500 = 1500$
 - $\text{tokens} = \text{committed_rate} * \text{td} = 2000 * 1 = 2000$
 - $2000 > 1500$. The tokens are greater than the actual debt.
Because tokens are greater than the actual debt, the user has been idle for a sufficient amount of time and the packet is transmitted.
- The second packet in this example is 1500 bytes and arrives 1/4 of a second later.
 - The packet size is 1500.
 - The td is 1/4 of a second.
 - $\text{actual_debt} = 0 + 1500 = 1500$

**Note**

The previous actual debt is equal to 0 in this calculation because the amount of tokens was greater than the actual debt and the previous packet, therefore, was forwarded without using a burst.

Debt can only be incurred when a burst is used to forward a packet.

- $\text{tokens} = 2000 * 1/4 = 500$
- $500 < 1500$. The tokens are less than the actual debt, so tokens need to be borrowed to forward the packet.
- $\text{actual_debt} = \text{previous_actual_debt} - \text{tokens} = 1500 - 500 = 1000$
- $1000 < 3000$. Therefore, the actual debt is less than the normal burst size. The packet is forwarded, and the actual debt is now 1000.
- The third packet is 5000 bytes and arrives 1/2 of a second later.
 - The packet size is 5000.
 - The td is 1/2 of a second.
 - $\text{actual_debt} = 1000 + 5000 = 6000$
 - $\text{tokens} = 2000 * 1/2 = 1000$
 - $1000 < 6000$. The tokens are less than the actual debt, so tokens need to be borrowed to forward the packet.
 - $\text{actual_debt} = 6000 - 1000 = 5000$
 - $5000 > 3000$. The actual debt is greater than the normal burst, so excess burst needs to be checked.
 - $\text{compound_debt} = \text{previous_compound_debt} + (\text{actual_debt} - \text{normal_burst}) = 0 + (5000 - 3000) = 2000$

- $2000 < 4000$. The compound debt is less than the excess burst size. Therefore, the packet is forwarded using the excess burst. After the packet is forwarded, the actual debt is at 5000 and the compound debt is at 2000.
- The next packet is 50 bytes and arrives 3 seconds later.
 - The packet size is 50 bytes.
 - The td is 3 seconds.
 - $actual_debt = 5000 + 50 = 5050$
 - $tokens = 2000 * 3 = 6000$
 - $6000 > 5050$. Therefore, the packet is forwarded without borrowing tokens.
 - The actual debt is reset to 0 because the generated tokens forwarded the packet. The user was idle for a sufficient period of time to forward the packet.
- The next packet is 10000 bytes and arrives 1/4 of a second later.
 - The packet size is 10000 bytes.
 - The td is 1/4 of a second.
 - $actual_debt = 0 + 10000 = 10000$
 - $tokens = 2000 * 1/4 = 500$
 - $500 < 10000$. Therefore, the tokens are less than the actual debt and tokens need to be borrowed.
 - $actual_debt = 10000 - 500 = 9500$
 - $9500 > 3000$. The actual debt is greater than the normal burst.
 - $compound_debt = 2000 + (9500 - 3000) = 8500$
 - $8500 > 4000$. The compound debt is greater than the excess burst. The packet is dropped.
 - After the packet is dropped, the compound debt is reset.
 - $actual_debt = previous_actual_debt - packet\ size = 9500 - 10000 = -500$. The actual debt cannot be a negative number, so it is set at 0.

Future packets will continue to get forwarded based on the algorithm.

Per-Session Policing Example

In the following example, a RADIUS service profile is configured for per-session policing.

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "QU16000:3000:4000:D24000:4000:8000"
```

The router also must be configured to enable policing configurations in RADIUS service profiles. To enable per-session policing on a router, the following command must be entered:

```
Router(config)# ssg qos police session
```

For information on how this service profile traffic will be policed, see the [“Per-User Policing with Excess Burst Example”](#) section. The service profile traffic will be policed identically to the traffic in that section, with the exception that the service profile traffic is being policed.

Verifying a Policing Configuration Example

The **show ssg host** command is used to verify if per-user policing is enabled.

In the following sample **show ssg host** command output, SSG Hierarchical Policing is enabled for upstream and downstream traffic. The output related to SSG Hierarchical Policing has been italicized for emphasis.

```
router> show ssg host 128.0.0.0
----- HostObject Content -----
Activated:TRUE
Interface:
User Name:jdoo
Host IP:128.0.0.0
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
Qos Upstream Parameters
CIR(bps) = 8000, Normal Burst(bytes) = 4000 Excess Burst(bytes) = 5000
Qos Downstream Parameters
CIR(bps) = 16000, Normal Burst(bytes) = 5000 Excess Burst(bytes) = 6000
User logged on since:*20:54:44.000 UTC Sun Nov 25 2001
User last activity at:*20:54:50.000 UTC Sun Nov 25 2001
SMTP Forwarding:NO
Initial TCP captivate:NO
TCP Advertisement captivate:NO
Default Service:NONE
DNS Default Service:NONE
Active Services:NONE
```

In the following **show ssg host** command output, SSG Hierarchical Policing is disabled. The line indicating that SSG Hierarchical Policing has been disabled is italicized for emphasis.

```
router> show ssg host 128.0.0.0
----- HostObject Content -----
Activated:TRUE
Interface:
User Name:jdoo
Host IP:128.0.0.0
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:*20:54:44.000 UTC Sun Nov 25 2001
User last activity at:*20:54:51.000 UTC Sun Nov 25 2001
SMTP Forwarding:NO
Initial TCP captivate:NO
TCP Advertisement captivate:NO
Default Service:NONE
DNS Default Service:NONE
Active Services:NONE
AutoService:NONE
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [attribute](#)
- [ssg qos police](#)

attribute

To configure an attribute in a local service profile, use the **attribute** profile configuration command. Use the **no** form of this command to delete an attribute from a service profile.

attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

no attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

Syntax Description

<i>radius-attribute-id</i>	RADIUS attribute ID to be configured.
<i>vendor-id</i>	(Optional) Vendor ID. Required if the RADIUS attribute ID is 26, indicating a vendor-specific attribute. The Cisco vendor ID is 9.
<i>cisco-vsa-type</i>	(Optional) Cisco vendor-specific attribute (VSA) type. Required if the vendor ID is 9, indicating a Cisco VSA.
<i>attribute-value</i>	Attribute value.

Defaults

No default behavior or values.

Command Modes

Profile configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(4)B	The Q attribute was introduced as an <i>attribute-value</i> .
12.2(13)T	The Q attribute was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to configure attributes in local service profiles.

For the SSG Open Garden feature, use this command to configure the Service Route, DNS Server Address, and Domain Name attributes in a local service profile before adding the service to the open garden.

For the SSG Hierarchical Policing feature, use the Q option to configure the token bucket parameters (token rate, normal burst, and excess burst). The syntax for the Q parameter:

```
Router(config-prof)# attribute radius-attribute-id vendor-id cisco-vsa-type
"QU;upstream-committed-rate;upstream-normal-burst;
[upstream-excess-burst];D;downstream-committed-rate;
downstream-normal-burst;[downstream-excess-burst]"
```

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. See the “[SSG Hierarchical Policing Token Bucket Scheme](#)” section of this document for additional information on how these parameters police traffic.

Examples

In the following example, the Cisco-AVpair Upstream Access Control List (inacl) attribute is configured in the local service profile called cisco.com:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "ip:inacl#101=deny tcp 10.2.1.0 0.0.0.255 any eq 21"
```

In the following example, the Session-Timeout attribute is deleted from the local service profile called cisco.com:

```
Router(config)# local-profile cisco.com
Router(config-prof)# no attribute 27 600
```

In the following example, the SSG Hierarchical Policing parameters are set for upstream and downstream traffic:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 251 "QU:8000:16000:20000:D10000:20000:30000"
```

In the following example, an open garden service called opencisco.com is defined.

```
Router(config)# local-profile opencisco.com
Router(config-prof)# attribute 26 9 251 "Oopengarden1.com"
Router(config-prof)# attribute 26 9 251 "D10.13.1.5"
Router(config-prof)# attribute 26 9 251 "R10.1.1.0;255.255.255.0"
Router(config-prof)# exit
Router(config)# ssg open-garden opencisco.com
```

Related Commands

Command	Description
local-profile	Configures a local service profile.
show ssg open-garden	Displays a list of all configured open garden services.
ssg open-garden	Designates a service, defined in a local service profile, to be an open garden service.
ssg qos police	Enables SSG Hierarchical Policing on a 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. The show ssg host command should be used to verify per-user policing.
show ssg connection	Displays information about a particular SSG connection, including the policing parameters.
debug ssg data	Displays SSG QoS information.

ssg qos police

To enable the limiting transmission rates for an SSG subscriber or for a service being used by an SSG subscriber, use the **ssg qos police** command in global configuration mode. To disable the limiting of transmission rates, use the **no** form of this command.

ssg qos police [user | session]

no ssg qos police [user | session]

Syntax Description

user	Specifies per-user policing. Per-user policing is used to police bandwidth allocations for separate subscribers of an SSG service.
session	Specifies per-session policing. Per-session policing is used to police the bandwidth used by one subscriber for multiple services.

Defaults

No default behavior or values. Traffic is forwarded with no SSG policing restrictions if the **ssg qos police** command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command enables the SSG Hierarchical Policing feature, which is used to limit the output transmission rate for a subscriber or for a specific SSG service used by a subscriber. The parameters used to police traffic (committed rate, normal burst, and excess burst) are configured in a RADIUS user profile (per-user policing) or a RADIUS service profile (per-session policing) by using the Q option.

Examples

The examples for SSG Hierarchical Policing require configuration steps as well as examples of how sample traffic is policed based on a policing configuration. Therefore, these examples are lengthy and detailed.

These examples can be viewed in the [“Configuration Examples”](#) section of this document.

Related Commands

Command	Description
attribute	Specifies the attributes of a service profile for SSG. The parameters that are used by the token bucket to police traffic are specified using the attribute command.
show ssg host	Displays information about an SSG host, including whether policing is enabled or disabled and the policing configurations of a particular host. The show ssg host command should be used to verify per-user policing.
show ssg connection	Displays information about a particular SSG connection, including the policing parameters.
debug ssg data	Displays SSG QoS information.

