Configuring the SSG for SESM Deployments

This appendix shows the minimum required configuration for the Cisco Service Selection Gateway (SSG) to work with a Subscriber Edge Services Manager (SESM) deployment.

For more information about configuring SSG, including optional features and more explanation of the required configurations described in this appendix, see the SSG documentation. The "Related Documentation" section in the preface of this guide includes an online link to SSG documentation.

Basic SSG Configuration

This section shows the required commands for configuring SSG to work with SESM portals.

Step 1 To enable the SSG, enter:

```
ip cef
ssg enable
```

The Cisco Express Forwarding (CEF) feature is required for SSG.

Step 2 To identify the network where the SESM portal is running, enter:

ssg default-network *IPaddress mask*

where *IPaddress* and *mask* identify the network where the SESM portal is running.

Step 3 To configure the port on which the SSG will listen for SESM requests, enter:

ssg radius-helper auth-port *port*

where *port* is the port on which all requests from SESM portals arrive. The default port used in SESM configurations is 1812.

Step 4 To specify the shared secret for password encryption between SSG and the SESM portal, enter:

ssg radius-helper key *password*

where *password* matches the password configured on the SESM portal. The default password used in SESM configurations is cisco.

Step 5 To have the SSG cache subscriber profiles obtained during authentication, enter:

ssg profile-cache

In SESM RADIUS mode deployments, profile caching is required. The subscriber profiles are included in access-accept replies to authentication requests. The SSG must cache the profile obtained during the authentication stage to make the profile available later when the SESM application queries the SSG.

For SESM LDAP mode deployments, profile caching is not required. Subscriber profiles are obtained from the directory separately from the authentication stage. The memory saved by turning off the profile caching increases the scalability of the SSG host device.

Step 6 To configure the SSG to perform RADIUS authentication, the minimum configuration is:

```
aaa new-model
aaa authentication login default none
aaa authentication ppp default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa session-id common
```

Note In LDAP mode, the RADIUS server is the SESM RADIUS Data Proxy (RDP) server.

Step 7 To configure communication between SSG and the RADIUS server, enter:

radius-server host *ipAddress* **auth-port** *authPort* **acct-port** *acctPort* **key** *password*

where:

ipAddress is the address of the RADIUS server. In LDAP mode, this is the address of the RDP.

authPort is the port SSG uses for authentication requests. The standard is 1812.

acctPort is the port SSG uses for accounting requests. This is optional in SESM deployments. The standard is 1813.

password is the RADIUS shared secret for password encryption

Step 8 To specify the password that SSG uses to query the RADIUS server for service profiles, enter:

ssg service-password service*ProfilePassword*

where *serviceProfilePassword* matches the password in the service profiles. The default password used in SESM configurations and sample data files is servicecisco.

Step 9 Every service must be bound to an uplink interface. If the service binding is not defined in the next-hop table on the SSG device, then the service must be bound by using the **ssg bind service** command.

Step 10 (Optional but recommended) Configure the SSG port-bundle host key feature as described in the following section.

Configuring the Port-Bundle Host Key Feature on SSG

For the host key port bundle mechanism to operate correctly, the SESM web application must reside in the default network with subscribers (PPP or bridged/routed) connected on downstream interfaces.

Note The host key feature requires Cisco IOS Release 12.2(2)B or later on the SSG device.

To configure the SSG for host key operation, enter the following configuration commands at the terminal configuration prompt on the SSG host:

```
ssg port-map enable
ssg port-map source ip loopback 0
ssg port-map destination range lowPort to highPort ip SESMaddress
```

The **ssg port-map source ip** command configures the IP addresses for use as the IP portion of the host key. Each configured address allows for approximately 4000 host keys, if the default port bundle length of 4 is used. This address becomes the source IP address for all upstream TCP packets from SSG to the SESM web application (and conversely, the destination address for all downstream TCP packets from the SESM web application to the SSG). Although you can explicitly configure these addresses, the safest way to configure them is by using a loopback interface, as shown above, because these IP addresses must be recognized as corresponding to a local interface or loopback.

Note If you use the interface that is configured to give SSG access to the default network as one of the interfaces in the **ssg port-map source ip** command, that interface cannot also be used as a Telnet interface into the SSG host.

The **ssg port-map destination range** command defines the address and ports of the SESM web application, where:

lowPort is the lowest SESM port

highPort is the highest SESM port

SESMaddress is the IP address of SESM

If there is only one SESM port available, *highPort* should have the value *lowPort* + 1. For example:

```
ssg port-map destination range 10100 to 10101 ip 10.0.3.1
```

Sample SSG Configuration

The following annotated configuration example shows how to configure SSG to work with SESM applications.

```
c7200-1#sho run
Building configuration...

Current configuration : 4499 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c7200-1
!
boot system flash disk0:c7200-g4js-mz.v122_4_b_throttle
```

The following lines configure AAA authentication.

```
aaa new-model
!
!
aaa authentication login default none
aaa authentication ppp default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa session-id common
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
!
```

```
!ip cef
!
!
```

The following lines enable and configure SSG to communicate with the SESM web application.

```
!!
ssg enable

ssg default-network 192.168.254.16 255.255.255.248
ssg service-password servicecisco
ssg radius-helper auth-port 1812
ssg radius-helper key cisco
ssg accounting interval 999999
ssg profile-cache
```

The following lines configure the SSG port-bundle host key feature.

```
ssg port-map enable
ssg port-map destination range 8080 to 8080 ip <sesmIPaddress>
ssg port-map destination range 8443 to 8443 ip <sesmIPaddress>
>
ssg port-map source ip Loopback0
!
!
ssg bind service passthrough1 FastEthernet4/0
ssg bind service proxy1 FastEthernet4/0
ssg bind service tunnel1 FastEthernet4/0
ssg bind direction downlink FastEthernet1/0
ssg bind direction downlink Ethernet3/2
!
```

The following lines configure a RADIUS proxy server.

```
ssg radius-proxy
 client-address 192.167.254.26 key cisco
 address-pool 10.0.0.1 10.0.0.200
!
```

The following lines configure SSG TCP redirections.

```
ssg tcp-redirect
 network-list Unauth-Service-pass
  network 10.60.60.0 255.255.255.128
 !
 network-list Unauth-Service-prox
  network 10.61.61.0 255.255.255.128
 !
 network-list Unauth-Service-tunn
  network 10.62.62.0 255.255.255.128
 !
 port-list ports
  port 80
  port 8080
 !
 server-group Unauth-User
  server 192.168.254.21 8090
 !
 server-group Initial
  server 192.168.254.21 8091
 !
 redirect port-list ports to Initial
 !
 server-group Advertisment
  server 192.168.254.21 8092
 !
```

```
 redirect port-list ports to Advertisment
 !
 server-group Unauth-Service-pass
  server 192.168.254.21 8094
 !
 redirect port-list ports to Unauth-Service-pass
 redirect unauthorized-service destination network-list Unauth-Service-pass to

Unauth-Service-pass
 !
 server-group Unauth-Service-prox
  server 192.168.254.21 8095
 !
 redirect port-list ports to Unauth-Service-prox
 redirect unauthorized-service destination network-list Unauth-Service-prox to


Unauth-Service-prox
 !
 server-group Unauth-Service-tunn
  server 192.168.254.21 8096
 !
 redirect port-list ports to Unauth-Service-tunn
 redirect unauthorized-service destination network-list Unauth-Service-tunn to


Unauth-Service-tunn
 !
 server-group Advertisement
 !
 redirect unauthenticated-user to Unauth-User
 redirect captivate initial default group Initial duration 1
 redirect captivate advertising default group Advertisment duration 5 frequency 600
!
!
```

The following lines configure the device interfaces.

```
interface Loopback0
 ip address 10.2.2.1 255.255.255.0
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.0.3.20 255.255.255.128
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface FastEthernet1/0
 ip address 192.168.254.25 255.255.255.248
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface ATM2/0
 no ip address
 no ip mroute-cache
 shutdown
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
!
interface Ethernet3/0
 ip address 10.10.10.1 255.255.255.0
 no ip mroute-cache
 duplex half
```

```
 no cdp enable
!
interface Ethernet3/1
 ip address 192.168.254.20 255.255.255.248
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet3/2
 ip address 192.168.254.4 255.255.255.248
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet3/3
 ip address 10.5.5.2 255.255.255.0
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface FastEthernet4/0
 ip address 172.16.59.1 255.255.255.0
 no ip mroute-cache
 duplex half
 no cdp enable
!
ip default-gateway 192.168.254.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.52.199.1
ip route 10.0.12.0 255.255.255.128 10.10.10.2
ip route 10.1.0.0 255.255.0.0 10.0.4.1
ip route 10.50.0.0 255.255.0.0 10.52.199.1
ip route 192.168.254.100 255.255.255.255 10.52.199.1
ip route 172.19.60.0 255.255.255.128 10.59.59.2
ip route 172.18.61.0 255.255.255.128 10.59.59.2
ip route 172.17.62.0 255.255.255.128 10.59.59.2
ip route 172.16.70.0 255.255.255.0 10.59.59.2
ip route 192.168.0.0 255.255.0.0 10.52.199.1
no ip http server
ip pim bidir-enable
!
```

The following lines configure communication between SSG and a RADIUS server.

```
radius-server host 192.168.254.100 auth-port 1812 acct-port 1813 timeout 10 retransmit 3
key cisco
radius-server retransmit 3
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
call rsvp-sync
!
mgcp profile default
dial-peer cor custom
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
end
c7200-1#
```