APPENDIX B

Configuring the SSG

This appendix illustrates some basic steps for configuring the Cisco Service Selection Gateway (SSG) to work with a Subscriber Edge Services Manager (SESM) web application. For a complete description of how to configure SSG, see the following documentation:

- *Cisco 6400 Feature Guide*—This guide includes a chapter that documents SSG features. The online link to this guide is:

  http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/feat_gd/12_1_5/index.htm

- *Cisco 6400 Command Reference*—This guide includes a chapter that defines SSG configuration commands. The online link to this guide is:

  http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/commandr/index.htm

- *Cisco 6400 NRP—Release Notes for Cisco IOS Release 12.1(5)DC*—The online link to these release notes is:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121relnt/6400/rn121dc5.htm

Basic SSG Configuration

This section shows basic procedures for enabling an SSG and configuring it to communicate with a RADIUS server. When following these procedures, replace the sample IP addresses, port numbers, and passwords with values that are appropriate for your configuration.

Step 1 Log on to the NRP.

Step 2 To access enabled mode, enter:

```
en
```

Step 3 To change the configuration, enter:

```
conf t
```

Step 4 To enable the SSG, enter:

```
ssg enable
```

Step 5 To remove a line, enter:

```
no radius-server host 10.3.3.2 auth-port 1647 acctport 1648 0 key cisco
```

Step 6 To add an entry, enter:

```
radius-server host 10.3.3.2 auth-port 1812 acctport 1813 0 key cisco
```

Step 7 To end editing, enter:

```
Ctrl-Z
```

Step 8 To rebuild the configuration, enter:

```
wr t
```

Step 9 To examine the current configuration, enter:

```
show run
```

Step 10 The relevant configuration entries are as follows:

a. To identify the network that the SESM web application is running on, enter:

```
ssg default-network 10.3.3.0 255.255.255.0
```

b. To specify the password to query RADIUS for service profiles, enter:

```
ssg service-password servicecisco
```

c. To configure the RADIUS protocol communication used between SSG and the SESM web application, specify the port on which the SSG is listening as follows:

```
ssg radius-helper auth-port 1812
```

d. To specify the shared secret for password encryption between SSG and the SESM web application, enter:

```
ssg radius-helper key cisco
```

e. To specify the maximum number of concurrent services for a user, enter:

```
ssg maxservice 21
```

f. To configure communication between SSG and the RADIUS server, specify the authentication port, the accounting port, and the secret as follows:

```
radius-server host 10.3.3.2 auth-port 1812 acct-port 1813 key cisco
```

g. To specify the number of RADIUS retries for authentication, enter:

```
radius-server retransmit 3
```

h. To specify the shared secret for password encryption to the RADIUS server, enter:

```
radius-server key cisco
```

Configuring the Host Key Port Bundle 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.

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.

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 implement the following features:

- Enable and configure SSG
- Configure open gardens
- Configure TCP redirection
- Configure communication between SSG and a RADIUS server
- Configure communication between SSG and an SESM web application

Note The following sample SSG configuration is generated on a system running Cisco IOS Release 12.1(5)DC. The syntax for some SSG commands might change in a later Cisco IOS release.

```
#!
#! Last configuration change at 03:16:44 PST Thu May 17 2001 by cisco
#! NVRAM config last updated at 03:02:39 PST Thu May 17 2001 by cisco
#!
#version 12.1
#no service single-slot-reload-enable
#no service pad
#service timestamps debug datetime
#service timestamps log uptime
#no service password-encryption
#!
#hostname agg1-nrp8
```

```
#!
#boot system flash:c6400r-g4p5-mz.121-5.DC.bin
#logging rate-limit console 10 except errors
#no logging console
#aaa new-model
#aaa authentication banner ^C !!! Cisco 6400 NRP8 Service Selection Gateway !!! ^C
#aaa authentication fail-message ^C Unauthorized Access Is Not Permitted ^C
#aaa authentication password-prompt Password:
#aaa authentication username-prompt Username:
#aaa authentication login console local
#aaa authentication ppp default local group radius
#aaa authorization network default local group radius
#aaa accounting update periodic 300
#aaa accounting network default start-stop group radius
#aaa nas port extended
#enable password zeus
#!
#username cisco password 0 cisco
#!
```

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

```
#ssg enable
#ssg default-network 192.168.2.0 255.255.255.0
#ssg service-password xssg-key
#ssg radius-helper auth-port 1812 acct-port 1813
#ssg radius-helper key cisco
#ssg next-hop download ssg-next-hop xssg-key
#ssg accounting interval 600
#ssg bind service internet FastEthernet0/0/0
#ssg bind service opengarden-aggregation FastEthernet0/0/0
#ssg bind service proxy ATM0/0/0.2
#ssg bind direction downlink ATM0/0/0.301
#ssg bind direction uplink FastEthernet0/0/0
#ssg bind direction uplink ATM0/0/0.2
#ssg bind direction downlink ATM0/0/0.3
```

The following lines illustrate how to configure SSG open gardens:

```
#ssg open-garden opengarden-aggregation
#ssg open-garden opengarden-microweb
#ssg open-garden opengarden-xyz.com
#ssg service-search-order local remote
#!
#local-profile opengarden-microweb
# attribute 26 9 251 "R10.1.1.100;255.255.255.255"
# attribute 26 9 251 "D10.1.2.133"
# attribute 26 9 251 "Ocisco.com"
#!
#local-profile opengarden-xyz.com
# attribute 26 9 251 "R10.1.1.0;255.255.255.255"
# attribute 26 9 251 "D10.1.1.10"
# attribute 26 9 251 "Oxyz.com;zap.com"
#!
#local-profile opengarden-aggregation
# attribute 26 9 251 "D192.1.1.10"
# attribute 26 9 251 "Ocisco.com"
# attribute 26 9 251 "R11.1.1.99;255.255.255.255"
#!
```

The following lines illustrate how to configure the TCP redirect capability. The http-redirect group command specifies an arbitrary name for a captive portal group. You can define multiple captive portal groups, each one directing a set of subscribers to different SESM web applications.

This example defines one captive portal group (captive-portal-1) that is serviced by the SESM web application running on server 10.1.2.50, port 80. The following incoming requests are redirected to that SESM application:

- Subscribers attempting to connect on port 81 get redirected.
- Subscribers attempting to connect from the network defined by IP address 192.168.10.0, mask 255.255.255.0.
- All unauthorized subscribers (that is, subscribers who have just opened their browsers and are not yet logged into SESM are redirected. Regardless of the URL they specify when they open their browsers, they are redirected to the SESM application first.

The lines below imply that the SESM application on server 10.1.2.50, port 80 is configured with the captive portal option turned on and that a captive portal application is running. The SESM application's related captive portal application examines the captured packet and determines an appropriate action. The captive portal application could authenticate the subscriber and display the list of authorized services, or it might display an SESM logon page. Another possibility is that the captive portal application could authenticate the subscriber and then redirect the packet to the original URL the subscriber specified. For example, the captive portal application might honor the home page specified in the subscriber's browser.

```
#ssg http-redirect group captive-portal-1 server 10.1.2.50 80
#ssg http-redirect port 81 group captive-portal-1
#ssg http-redirect network 192.168.10.0 255.255.255.0 group captive-portal-1
#ssg http-redirect unauthorized-user group captive-portal-1
#!
#!

#interface Ethernet0/0/1
# no ip address
#!
#interface Ethernet0/0/0
# description Management LAN
# ip address 192.168.2.48 255.255.255.0
#interface FastEthernet0/0/0
# ip address 192.168.1.48 255.255.255.0
# full-duplex
#!
```

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

```
#ip radius source-interface Ethernet0/0/0
#!
#radius-server configure-nas
#radius-server host 192.168.2.50 auth-port 1812 acct-port 1813
#radius-server retransmit 3
#radius-server timeout 60
#radius-server deadtime 2
#radius-server attribute 25 nas-port format d
#radius-server attribute nas-port format d
#radius-server key cisco
#radius-server vsa send accounting
#radius-server vsa send authentication
```