



Node Route Processor—Service Selection Gateway Enhancements V

This document describes further enhancements to the Node Route Processor—Service Selection Gateway (NRP-SSG) features in Cisco IOS Release 12.1(5)DC, and includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 3
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 3
- Command Reference, page 7
- Glossary, page 16

Feature Overview

The enhancements described in this document are included in Cisco IOS Release 12.1(5) DC. The NRP-SSG feature was first released in Cisco IOS Release 12.0(3) DC, and enhancements were added in Cisco IOS Releases 12.0(5) DC, 12.0(7) DC, 12.1(1)DC, and 12.1(3) DC.

The NRP-SSG is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using high-speed data circuit equipment (DCE) such as asymmetric digital subscriber line (ADSL) to allow simultaneous access to network services. The NRP-SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD), a web-based server application that allows users to select from multiple passthrough and proxy services through a standard web browser.

HTTP Redirect

The Hypertext Transfer Protocol (HTTP) Redirect feature works in conjunction with the Cisco Service Selection Dashboard (SSD) to implement captive portals: If a user has not logged in and sends packets upstream to a configurable group of TCP ports, SSG sends those packets to a captive portal group (one or more servers). The SSD handles the incoming packets in a suitable manner, such as returning a login page.

The group of captive portals consists of one or more SSDs. The SSG redirects packets to the captive portal groups on a round-robin basis.

The HTTP Redirect feature provides a means for user authentication without requiring the user to know the dashboard URL. It enables service providers to implement captive portals, own the user experience, advertise value-added services, and build a brand experience.

**Note**

HTTP Redirect is supported in 12.1(5)DC for bridged or routed users. It supports subscribers coming in on bridged or routed interfaces. This feature does not support subscribers coming in with PPP and RBE. SSG operates using standard Internet protocols with AAA and other Web servers the user chooses. A customer can currently use any Web server that can handle the HTTP Redirect. Cisco SSD version 3.0 can receive HTTP Redirection from SSG and handles the request. Release 3.0(1) of the SSD, which is scheduled to FCS in June 2001.

Open Garden

An Open Garden is one or more domains that can be accessed without user authentication. This differs from a “Walled Garden”. A “Walled Garden” refers to a collection of Web sites, or networks in general, that a user can access after providing minimal authentication information.

The Open Garden enhancement enables a list of as many as 100 domains to be associated with the default network. If a subscriber creates a DNS request for one of those domain names, the DNS request is resolved by the SSG to the default network. This ensures that a subscriber can access the Service Selection Dashboard, which typically resides on the management network with a private address, even when the subscriber is assigned a public DNS server.

Benefits

HTTP Redirect

- Provides a means for user authentication without the user needing to know the dashboard URL.
- Enables the provider to implement a captive portal, own the user experience, advertise value-added services, and build a brand experience.

Open Garden

- Subscriber can access a limited number of Web sites without logging into the network.
- Administrator can configure which sites a nonauthenticated user is allowed to access.

Restrictions

The HTTP Redirect feature requires Service Selection Dashboard, Release 3.0(1) to implement captive portal capability.

The software does not support binding two services to the same interface. If a configuration has open garden and proxy service bound to the same interface, the open garden functionality will fail.

Related Features and Technologies

Related Documents

- *Cisco 6400 Software Configuration Guide and Command Reference*
- *Node Route Processor—Service Selection Gateway* feature module
- *Node Route Processor—Service Selection Gateway Enhancements* feature module
- *Node Route Processor—Service Selection Gateway Enhancements II* feature module
- *Node Route Processor—Service Selection Gateway Enhancements III* feature module
- *Node Route Processor—Service Selection Gateway Enhancements IV* feature module
- Cisco Service Selection Dashboard documentation

Supported Platforms

- Cisco 6400 node route processor 1 (NRP-1) and node route processor 2 (NRP-2).

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

RFCs

No new or modified RFCs are supported by these features.

Prerequisites

In order to use these new features, you must install and configure Cisco SSD Version 2.5 or higher. For HTTP Redirect, Version 3.0(1) is required.

Configuration Tasks

Configuring an Open Garden

To configure an open garden:

1. Create a local profile for each open garden network desired.

- Specify the networks available to the user
 - Specify the available domains
 - Specify the DNS IP address in the open garden network.
2. Add this new profile to the open garden list.

Creating a Local Profile for an Open Garden

Use the **local-profile** *profile-name* command to enter profile configuration mode and to create and name a local profile.

Syntax Description

<i>profile-name</i>	User-defined name for the open garden network.
---------------------	--

Example

```
Router# local-profile opengarden_network1
```

Use the **attr** *radius-attribute-id* [*vendor-id*] [*cisco-vs-a-type*] *attribute-value* command to define the local profile attributes R,O,D, where networks and domain names can be configured for each open garden network.

Syntax Description

R	Open garden network IP address and subnet mask.
O	Domain names list.
D	DNS IP address.

Table 1 lists VSAs (vendor-specific attributes) used by the NRP-SSG. The vendor ID for all Cisco-specific attributes is 9.

Table 1 VSAs Related to NRP-SSG Support of the Proxy RADIUS Server

AttrID	Vendor ID	SubAttrID	SubAttrName	SubAttrDataType
26	9	251	Service-Info	String

Example

```
Router(opengarden_network1)# attribute 26 9 251 "R x.x.x.x;m.m.m.m"
Router(opengarden_network1)# attribute 26 9 251 "O www.cisco.com "
Router(opengarden_network1)# attribute 26 9 251 "D x.x.x.x"
```

Adding the Local Profile to the Open Garden List

Use the **ssg open-garden** *profile-name* command to add the new profile to the list of open garden networks.

Syntax Description

<i>profile-name</i>	The previously-defined name for the open garden network.
---------------------	--

Example

```
Router# ssg open-garden opengarden_network1
```

Verifying the Open Garden Configuration

-
- Step 1** To verify the open garden configuration, use the **show ssg open-garden *profile-name*** command and check for the open garden network statements in the output.

```
Router# show ssg open-garden opengarden_network1
```

Configuring HTTP Redirection

To configure HTTP redirection:

-
- Step 1** Define a captive portal group
 - Step 2** Add a TCP port to the portal group
 - Step 3** Set a default group for redirection of unauthorized users
-

Defining a Captive Portal Group

To define a group of one or more servers that make up the captive portal group, use the **ssg http-redirect group *group-name* server *ip-address* *port*** command.

Syntax Description

group	Defines a portal group.
<i>groupname</i>	The user-defined name for the captive portal group.
server	Adds a server to the group
<i>ip-address</i>	Specifies the IP address of the server to add to the group
<i>port</i>	TCP port on the server. Both <i>ip-address</i> and <i>port</i> are required.

Example

```
Router# ssg http-redirect group RedirectServer server 1.1.1.1 8080
```

Adding a TCP Port to the Portal Group

To add a TCP port to a list of ports that can be redirected by the captive portal group, use the **ssg http-redirect port *incoming destination port number* group *group-name*** command.

Syntax Description

port	Adds a TCP port to the list of redirectable ports.
<i>incoming destination port number</i>	The specific port number to add to the list.
group	Adds the specified port to the group specified in <i>group-name</i> .
<i>group-name</i>	Name of the portal group to which the port is added.

Example

```
Router# ssg http-redirect port 8080 group SSDGroup
```

Setting a Default Redirection Group

To select a captive portal group for redirection of traffic from an unauthorized user, use the **ssg http-redirect unauthorized-user group *group-name*** command.

Syntax Description

unauthorized-user	Adds a service to the list of redirectable services.
group	Select a portal group for traffic redirection from an unauthorized user.
<i>group-name</i>	Name of the portal group to which the traffic will be redirected.

Example

```
Router# ssg http-redirect unauthorized-user group SSDGroup
```

Verifying the HTTP Redirection

- Step 1** To verify that the HTTP redirection is set or to view any direct mappings, use the **show ssg http-redirect group [*name*]** command or the **show ssg http-redirect mappings [*ip-address*]** command and check for the HTTP redirect statements in the output.

If the **group** keyword is used and the optional *name* field is omitted, it displays a list of all defined portal groups. If the *name* field is included, it displays information about that group.

If the **mappings** keyword is used and the optional *ip-address* is omitted, then a list of IP addresses for all hosts with stored mappings is displayed. If the *ip-address* field is included, then any mappings for the host with that IP address is displayed.

```
Router# show ssg http-redirect
```

Troubleshooting Tips

To display all debug HTTP redirect information, use the **debug ssg http-redirect** command.

Example

```
Rouer# Debug ssg http-redirect
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- local-profile
- attr
- ssg open-garden
- show ssg open-garden
- ssg http-redirect
- show ssg http-redirect
- debug ssg http-redirect

local-profile

To enter profile configuration mode and to configure and name an open garden network, use the **local-profile** privileged EXEC command.

local-profile *profile-name*

no local-profile *profile-name*

Syntax Description	<i>profile-name</i>	User-defined name for an open garden network.
--------------------	---------------------	---

Defaults	This command has no default behavior.
----------	---------------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.0(3) DC	This command was introduced.
	12.1(5) DC	This command was modified.

Usage Guidelines	Use this command to create a local RADIUS profile and name for an open garden network.
------------------	--

attr

Use the **attr** *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value* command to define the local profile attributes R,O,D, where networks and domain names can be configured for each open garden network.

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

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

Syntax Description

<i>radius-attribute-id</i>	Number 26 indicates a Radius-specific attribute.
<i>vendor-id</i>	Number 9 specifies a Cisco-specific attribute.
<i>cisco-vsa-type</i>	Number 251 specifies an open garden network configuration
<i>attribute-value</i>	One of the three values below: R, O, or D.
R	Open garden network IP address and subnet mask.
O	Domain names list.
D	DNS IP address.

Table 2 lists VSAs (vendor-specific attributes) used by the NRP-SSG.

Table 2 VSAs Related to NRP-SSG Support of the Proxy RADIUS Server

AttrID	Vendor ID	SubAttrID	SubAttrName	SubAttrDataType
26	9	251	Service-Info	String

Defaults

This command has no default behavior.

Command Modes

Profile configuration

Command History

Release	Modification
12.1(5) DC	This command was introduced.

Usage Guidelines

Use this command to create a local RADIUS profile and name for an open garden network. The vendor ID for all Cisco-specific attributes is 9.

Examples

```
Router(opengarden_network1)# attribute 26 9 251 "R x.x.x.x;m.m.m.m"
Router(opengarden_network1)# attribute 26 9 251 "O www.cisco.com "
Router(opengarden_network1)# attribute 26 9 251 "D x.x.x.x"
```

ssg open-garden

To add the local RADIUS service profile that defines an open garden network to the list of open garden networks, use the **ssg open-garden** privileged EXEC command.

ssg open-garden *profile-name*

no ssg open-garden *profile-name*

Syntax Description

<i>profile-name</i>	The previously-defined name for an open garden network
---------------------	--

Defaults

This command has no default behavior.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5) DC	This command was introduced.

Usage Guidelines

Use this command to add the local RADIUS profile to the list of configured open garden networks.

show ssg open-garden

To display information about the configured open garden network, use the **ssg open-garden** privileged EXEC command.

```
show ssg open-garden profile-name
```

Syntax Description	<i>profile-name</i>	The previously-defined name for an open garden network
Defaults	This command has no default behavior.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.1(5) DC	This command was introduced.
Usage Guidelines	Use this command to view the configured open garden networks.	

ssg http-redirect

To define a group of one or more servers that make up the captive portal group and to configure http redirection to that portal group, use the **ssg http-redirect** command.

```

ssg http-redirect group <groupname> server <ip-address> <port> |
port <incoming destination port number> group <groupname> |
bind <service name> group <groupname>|
unauthorized-user group <groupname>|

```

group	Defines a portal group.
<i>group-name</i>	The user-defined name for the captive portal group.
server	Adds a server to the group.
<i>ip-address</i>	Specifies the IP address of the server to add to the group.
<i>port</i>	TCP port on the server. Both <i>ip-address</i> and <i>port</i> are required.
port	Adds a TCP port to the list of redirectable ports.
<i>incoming destination port number</i>	The specific port number to add to the list.
bind	Adds a destination service to the list of redirectable services.
<i>service name</i>	The specific service to add to the list.
unauthorized-user	Adds a service to the list of redirectable services.

Defaults

This command has no default behavior.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5) DC	This command was introduced.

Examples

```

Router#ssg http-redirect server group RedirectServer
server 10.1.1.1 8080
server 10.2.3.4 8081

```

This example puts two servers into group RedirectServer. The first is at IP address 10.1.1.1 and TCP port 8080, while the second is at 10.2.3.4 and port 8081.

```

Router#ssg http-redirect port 8080 group SSDGroup

```

The portal group SSDGroup is a candidate (also depends on the destination IP address) for redirection when a packet's destination TCP port is 8080.

```
Router#ssg http-redirect port IPTV group SSDGroup
```

The portal group SSDGroup is a possible candidate (also depends on the destination TCP port) for redirection when a packet's destination is the service IPTV.

```
Router#ssg http-redirect unauthorized-user group SSDGroup
```

The portal group SSDGroup is used for traffic from an unauthorized user.

show ssg http-redirect

To display information about the captive portal groups defined in the system, use the **show ssg http-redirect** privileged EXEC command.

```
show ssg http-redirect group [name]
```

```
show ssg http-redirect mappings [ip-address]
```

Syntax Description

group	Show group information.
<i>name</i>	The previously-defined name for the captive portal group.
mappings	Show internal redirection mappings
<i>ip-address</i>	Show redirection mappings for this specific host.

Defaults

If the **group** keyword is used and the optional *name* field is omitted, it displays a list of all defined portal groups. If the *name* field is included, it displays information about that group.

If the **mappings** keyword is used and the optional *ip-address* is omitted, then a list of IP addresses for all hosts with stored mappings is displayed. If the *ip-address* field is included, then any mappings for the host with that IP address is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5) DC	This command was introduced.

Usage Guidelines

Use this command to display information about the captive portal groups defined in the system.

Examples

```
router#show ssg http-redirect
router#show ssg http-redirect RedirectServer
```

The first example lists all the defined captive portal groups, the second displays a detailed description of the group RedirectServer.

debug ssg http-redirect

To turn on debug information for the HTTP redirect feature, use the **debug ssg http-redirect** privileged EXEC command.

debug ssg http-redirect

no debug ssg http-redirect

Defaults

This command has no default behavior.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(5) DC	This command was introduced.

Usage Guidelines

Use this command to turn on debug information for the HTTP redirect feature.

Examples

```
Router#Debug ssg http-redirect
```

Glossary

RADIUS—Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

VSA—vendor-specific attribute.