



SSG Default DNS Redirection

The SSG Default DNS Redirection feature allows a default Domain Name System (DNS) domain to be configured in a service profile. When a default DNS domain is configured in a service profile, all DNS queries that do not match a domain name will be redirected to the DNS server for that service.

Feature History for the SSG Default DNS Redirection Feature

Release	Modification
12.3(3)B	This feature was introduced.
12.3(7)T	This features was integrated into Cisco IOS Release 12.3(7)T.

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.

Contents

- [Prerequisites for SSG Default DNS Redirection, page 1](#)
- [Information About SSG Default DNS Redirection, page 2](#)
- [How to Configure SSG Default DNS Redirection, page 3](#)
- [Configuration Examples for SSG Default DNS Redirection, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)

Prerequisites for SSG Default DNS Redirection

Before Service Selection Gateway (SSG) default DNS redirection can be configured, SSG must be enabled by using the **ssg enable** command.



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Information About SSG Default DNS Redirection

To configure default DNS redirection for SSG, you should understand the following concepts:

- [DNS Redirection, page 2](#)
- [SSG Domain Name Attribute, page 2](#)

DNS Redirection

When SSG receives a DNS request, it performs domain name matching by using the Domain Name attribute from the service profiles of the currently logged-in services.

SSG default DNS redirection allows a default DNS domain to be configured in a service profile. When a default DNS domain is configured in a service profile, all DNS queries that do not match a domain name will be redirected to the DNS server for that service..

You can also configure the default domain to apply to DNS queries from unauthenticated users only. This configuration enables SSG to redirect all DNS queries for unauthenticated users to the Cisco Subscriber Edge Services Manager (SESM) DNS server, which can spoof the responses if required.

A domain name within the question section of the DNS packet is compared in sequence in the upstream path. The sequence is as follows:

1. The domain names configured in the logged-in services. If a match is found, the request is redirected to the DNS server for the matched service.
2. The domain names configured in the open garden service. If a match is found, the requested is redirected to the DNS server for the open garden service.
3. Default DNS domain (defined as an asterisk [*]) in a logged-in service.
4. Default DNS domain (defined as an asterisk [*]) in an open garden service.
5. If the user is logged in to a service that has Internet connectivity, the request is redirected to the first service in the user's service access order list that has Internet connectivity. Internet connectivity is defined as access to a service containing a Service Route attribute of 0.0.0.0/0.
6. If there is an open garden Internet service, the request is redirected to this service.
7. If a match is not found until now, the request is forwarded to the DNS server defined in the client's TCP/IP stack.

Default DNS redirection is useful in a public wireless LAN (PWLAN) environment in which a user's browser may be configured with a home page that is part of a corporate internal network. Since the home page domain will never be resolved by a DNS server in the Internet, the TCP session from the user will never be initiated. Default DNS redirection allows SSG to redirect all DNS queries to a DNS server that can resolve all queries—for example, the DNS server on the Cisco Subscriber Edge Services Manager (SESM), which can spoof all unresolved DNS queries.

SSG Domain Name Attribute

[Table 1](#) describes the Domain Name vendor-specific attribute (VSA) used by SSG. The Domain Name VSA specifies domain names that get DNS resolution from the DNS servers specified in the DNS server address.

Table 1 SSG Vendor-Specific Attribute for Domain Name

Attribute ID	Vendor ID	Subattribute ID and Type	Subattribute Name	Subattribute Data
26	9	251 Service-Info	Domain Name	<p>O{name1[;name2]...[;nameX] *[:unauthenticated]}</p> <p><i>name1</i>—Domain name that gets DNS resolution from this server.</p> <p><i>name2...x</i>—Additional domain names that get DNS resolution from this server.</p> <p>*—Default domain for all DNS queries. Note that this cannot be part of a list of domain names.</p> <p>*O;unauthenticated—Default domain will apply to DNS queries for unauthenticated users only. This is useful in a wireless LAN environment in which SSG redirects all DNS queries for unauthenticated users to the SESM DNS server, which can spoof the responses if required.</p> <p>Example: <code>ssg-service-info = "Ocisco.com;cisco-sales.com"</code></p> <p>Example: <code>ssg-service-info = "O*;unauthenticated"</code></p>

How to Configure SSG Default DNS Redirection

This section contains the following procedure:

- [Configuring SSG Default DNS Redirection in a Local Service Profile, page 3](#)

Configuring SSG Default DNS Redirection in a Local Service Profile

This task configures SSG default DNS redirection in a local service profile.

You can also configure SSG default DNS redirection by adding the VSA for default DNS redirection to the service profile on the RADIUS server. See the “[SSG Domain Name Attribute](#)” section on page 2 for information about the Domain Name VSA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **local-profile** *profile-name*
4. **attribute 26 9 251 "O*[:unauthenticated]"**
5. **end**
6. **show ssg service** [*service-name* [**begin** *expression* | **exclude** *expression* | **include** *expression*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>local-profile profile-name</code> Example: <code>Router(config)# local-profile og-dns</code>	Configures a local service profile and enters profile configuration mode.
Step 4	<code>attribute 26 9 251 "O*[,unauthenticated]"</code> Example: <code>Router(config-prof)# attribute 26 9 251 "O*"</code>	Configures the attribute for default DNS redirection in a local service profile.
Step 5	<code>end</code> Example: <code>Router(config-prof)# end</code>	(Optional) Returns to privileged EXEC mode.
Step 6	<code>show ssg service [service-name [begin expression exclude expression include expression]]</code> Example: <code>Router# show ssg service og-dns</code>	(Optional) Displays the information for about a service. <ul style="list-style-type: none">The output for this command indicates if default DNS matching is enabled and whether it is valid for unauthenticated users only.

Configuration Examples for SSG Default DNS Redirection

This section contains the following configuration examples:

- [SSG Default DNS Redirection: Example, page 4](#)
- [SSG Default DNS Redirection for Unauthenticated Users: Example, page 5](#)

SSG Default DNS Redirection: Example

In the following example, all DNS packets will be redirected to the DNS server 3.6.6.2.

```
! Define the service profile locally
local-profile og-dns
attribute 26 9 251 "D10.6.6.2"
attribute 26 9 251 "R10.6.6.2;255.255.255.255"
attribute 26 9 251 "O*"
!
```

```
! Make the service an open garden
ssg open-garden og-dns
```

When a default DNS domain is configured, the output for the **show ssg service** command will include the following line:

```
Default domain matching is Enabled
```

SSG Default DNS Redirection for Unauthenticated Users: Example

In the following example, default DNS matching is applied only to unauthenticated users. If the user is authenticated, the packet is processed normally.

```
! Define the service profile locally
local-profile og-dns-non-authen
  attribute 26 9 251 "D3.6.6.2"
  attribute 26 9 251 "R3.6.6.2;255.255.255.255"
  attribute 26 9 251 "O*;unauthenticated"
!
! Make the service an open garden
ssg open-garden og-dns-non-authen
```

When a default DNS domain is configured for unauthenticated users only, the output for the **show ssg service** command will include the following line:

```
Default domain matching is Enabled - valid only for unauthenticated users
```

Additional References

The following sections provide references related to SSG default DNS redirection.

Related Documents

Related Topic	Document Title
SSG commands	<i>Cisco IOS Wide-Area Networking Command Reference</i> , Release 12.3 T
SSG configuration tasks	“Broadband Access” section in the <i>Cisco IOS Wide-Area Networking Configuration Guide</i> , Release 12.3 SSG Features in Cisco IOS Release 12.3(4)T
SESM	<i>Cisco Subscriber Edge Services Manager</i> <i>Cisco Service Selection Dashboard</i>
RADIUS commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T
RADIUS configuration tasks	<i>Cisco IOS Security Configuration Guide</i> , Release 12.3

Standards

Standards	Title
No new or modified standards are supported by this feature. Support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature. Support for existing MIBs has not been modified by this feature.	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

RFCs	Title
No new or modified RFCs are supported by this feature. Support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 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/public/support/tac/home.shtml

Command Reference

This section documents the modified **show ssg service** command.

show ssg service

To display the information for a Service Selection Gateway (SSG) service, use the **show ssg service** command in privileged EXEC mode.

```
show ssg service [service-name [begin expression | exclude expression | include expression]]
```

Syntax Description	
<i>service-name</i>	(Optional) Name of an active Service Selection Gateway (SSG) service.
begin	(Optional) Begin with the line that contains <i>expression</i> .
<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Exclude lines that contain <i>expression</i> .
include	(Optional) Include lines that contain <i>expression</i> .

Defaults If no service name is provided, the command displays information for all services.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3) DC	This command was introduced on the Cisco 6400 node route processor.
	12.1(1) DC1	The output of this command was modified on the Cisco 6400 node route processor to display the following Service-Info Attributes when they are present in the proxy RADIUS service profile: <ul style="list-style-type: none"> • Service-Defined Cookie • Full Username Attribute
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.3(1a)BW	This command was modified to display the attribute filter that is set in the service profile.
	12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B. The output for this command was modified to display information about default DNS redirection.
	12.3(7)T	The modifications in Release 12.3(3)B were integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines Use this command to display connection information for a service.

Examples**L2TP Tunnel Service: Example**

The following example shows the information for the L2TP tunnel service called “tunnell”. The attribute filter that is set in the service profile can be seen in the output.

```
Router# show ssg service tunnell

----- ServiceInfo Content -----
Uplink IDB: gw: 0.0.0.0
Name: tunnell
Type: TUNNEL
Mode: CONCURRENT
Service Session Timeout: 0 seconds
Service Idle Timeout: 0 seconds
Service refresh timeleft: 99 minutes
No Authorization Required
Authentication Type: CHAP
Attribute Filter: 31
Session policing disabled
Reference Count: 1

DNS Server(s):
No Radius server group created. No remote Radius servers.

TunnelId: ssg1
TunnelPassword: cisco
HomeGateway Addresses: 172.0.0.1
ConnectionCount 1
Full User Name not used

Domain List: Included Network Segments:
              0.0.0.0/0.0.0.0

Active Connections:
      1 : RealIP=172.0.1.1, Subscriber=10.0.1.1

----- End of ServiceInfo Content -----
```

Proxy Service: Example

The following example shows information for the proxy service called “serv1-proxy”:

```
Router# show ssg service serv1-proxy

----- ServiceInfo Content -----
Uplink IDB:
Name:serv1-proxy
Type:PROXY
Mode:CONCURRENT
Service Session Timeout:0 seconds
Service Idle Timeout:0 seconds
Class Attr:NONE
Authentication Type:CHAP
Reference Count:1

Next Hop Gateway Key:my-key

DNS Server(s):Primary:10.13.1.5

Radius Server:IP=10.13.1.2, authPort=1645, acctPort=1646, secret=my-secret

Included Network Segments:
      10.13.0.0/255.255.0.0
```

```
Excluded Network Segments:
Full User Name Used
Service Defined Cookie exist
```

```
Domain List:service1.com;
```

```
Active Connections:
      1      :Virtual=255.255.255.255, Subscriber=10.20.10.2
```

```
----- End of ServiceInfo Content -----
```

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show ssg service Field Descriptions*

Field	Description
Uplink IDB	Interface through which the service is reachable.
Name	Service name.
Type	Type of service.
Mode	One of the following values: Concurrent—user can log into this service and other services simultaneously. Sequential—user cannot log into this service simultaneously with other services.
Service Session Timeout	Period of time after which the session (SSG connection) will be terminated.
Service Idle Timeout	If the session (SSG connection) is idle for this many seconds, the session will be terminated.
Service refresh timeleft	Amount of time after which SSG will refresh the service profile.
Authentication Type	Type of authentication that will be used for proxy or tunnel services. Values are PAP and CHAP.
Attribute Filter	RADIUS attribute that is being filtered out from user authentication.
Next Hop Gateway Key	Defines the next-hop binding. Services can be bound to the next hop using next-hop gateways. The key to next-hop-gateway mapping is present in the next-hop profile.
DNS Server(s)	DNS server used for this service.
TunnelId	ID for tunneling services.
TunnelPassword	Password for tunneling services.
HomeGateway Addresses	IP address of the LNS.

Table 2 show ssg service Field Descriptions (continued)

Field	Description
Radius Server: IP authPort acctPort secret	Information about the RADIUS server where proxy users are authenticated for service connectivity.
Included Network Segments	IP address subnets that form the service network.
Excluded Network Segments	IP address subnets that are excluded from the service network.
Full User Name Used	Indicates that the RADIUS authentication and accounting requests use the full username (user@service).
Service Defined Cookie exist	Indicates that user-defined information is included in RADIUS authentication and accounting requests.
Domain List	List of domain names that belong to the service and can be resolved by the DNS server specified for this service.
Active Connections Virtual Subscriber	Lists the host IP address for active connections. The subscriber IP address is the IP address of the host. In cases where there is a service-defined NAT, the virtual IP address is not zero and is the IP address given by the service.

Related Commands

Command	Description
clear ssg service	Removes a service.
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
ssg bind service	Specifies the interface for a service.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.