BLUE COAT®

ProxySG Appliance/ SGOS

Blue Coat Security First Steps

Transparent Proxy Deployments

Security Empowers Business

SGOS 6.5

Third Party Copyright Notices

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas:

Blue Coat Systems, Inc.

420 N. Mary Ave.

Sunnyvale, CA 94085

Rest of the World:

Blue Coat Systems International SARL

3a Route des Arsenaux

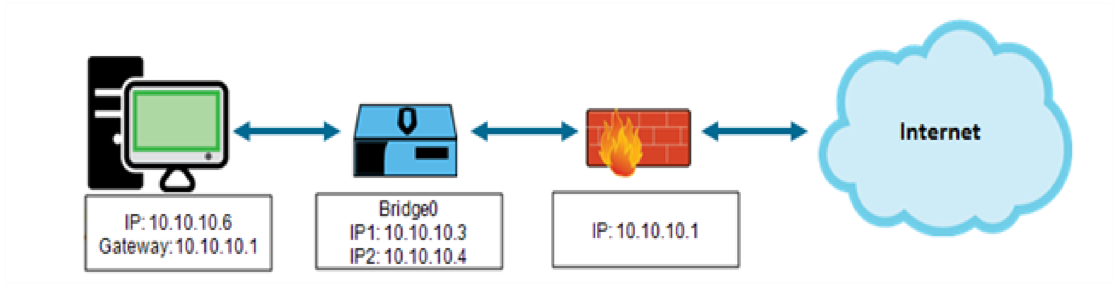
1700 Fribourg, Switzerland

Solution: Transparent Proxy Deployments

With a *transparent proxy* deployment, you can configure your ProxySG appliance to control and filter traffic for users, without having to do any configuration on the client workstations. Select one of the following methods to send traffic to your ProxySG appliance transparently.

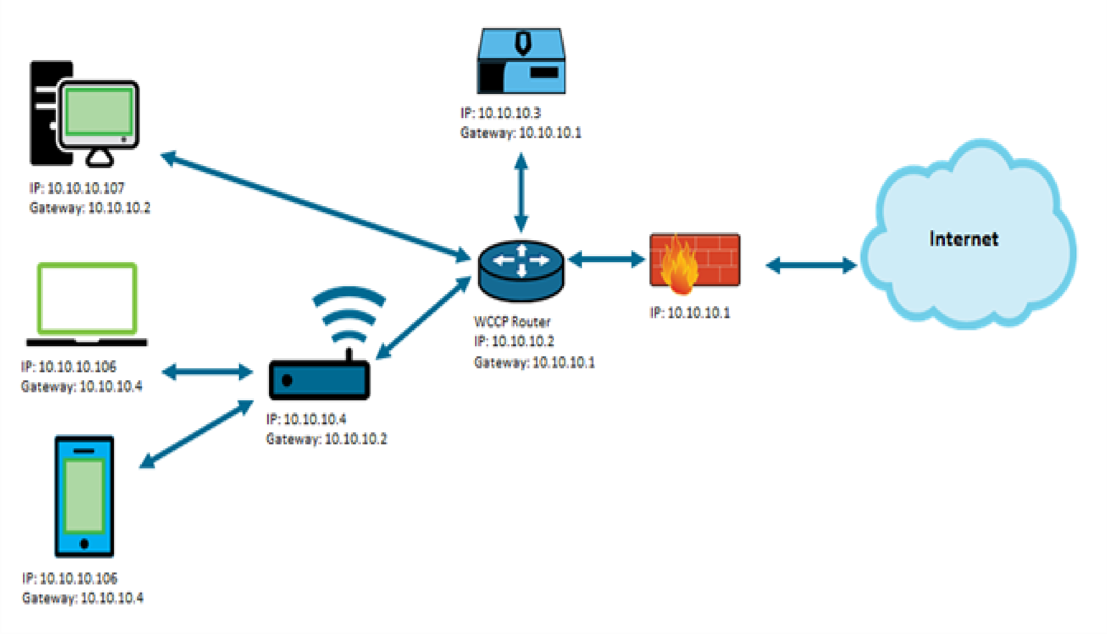
Physically in-path

This deployment method places the ProxySG appliance in the physical network path, between users and the Internet egress point, using two bridged interfaces on the appliance; these interfaces handle traffic without redirection. This deployment method ensures that the ProxySG appliance has the potential to control all user traffic destined for the Internet.



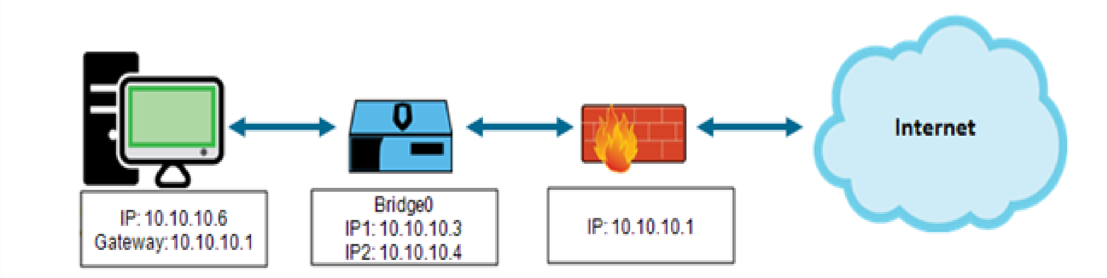
Virtually in-path: WCCP

Web Cache Control Protocol (WCCP) relies on Cisco and Cisco-compatible routers, firewalls, or switches that support the redirection of intercepted traffic to a cache control device, such as the ProxySG appliance. You can use WCCP to capture traffic destined for the Internet and redirect it to the ProxySG for processing and policy evaluation. WCCP provides options for balancing load among several ProxySG appliances and is fault tolerant, sending traffic to the Internet directly, should the ProxySG appliance be unable to handle requests.



Configure In-Path Proxy

An in-path transparent deployment allows the ProxySG appliance to handle all traffic flowing from your user network to the Internet. All traffic flows through the appliance, but only interesting traffic is processed and subjected to policy.



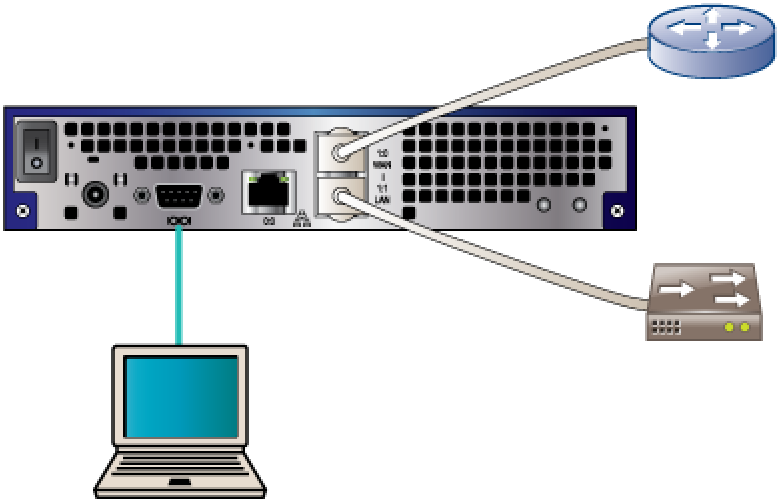
1. Connect the Bridged Interfaces.
2. Intercept User Traffic.
3. Configure the Default Proxy Policy .
4. Test Transparent Access.

Connect the Bridged Interfaces

Your ProxySG appliance has several types of network interfaces. Some appear as a single port, labeled 0:0, and others appear as two or four ports in a cluster, labeled 1:0, 1:1, and so on. In a physically in-path deployment, these bridged interfaces will continue to transmit data if the appliance ever loses power. When power is restored, the appliance manages traffic just as it did before power was lost.

> Tip This information is also provided in the Quick Start Guide poster, included with your ProxySG appliance. If you don't have your Quick Start Guide, you can find a PDF version by selecting your hardware model: https://bto.bluecoat.com/documentation/pubs/ProxySG

1. Connect your ProxySG appliance inline, between your user network and your firewall using a pair of bridged interfaces. Connect the LAN interface to your internal network and the WAN interface to your outbound network.



2. Connect a null-modem cable to the serial port at the rear of the appliance and to a computer with a terminal application such as Hyperterminal, Tera Term, or Putty. The terminal settings are as follows:
   - Baud rate: **9600 bps**
   - Parity: **none**
   - Flow control: **none**
   - Data bits: **8**
   - Stop bits: **1**
3. Power on the appliance and monitor the boot process in your terminal application. When prompted, select **Manual setup** and proceed with the **Other Solution** configuration wizard. This wizard will request the following information:
   - IP address and subnet mask for the primary passthru interface
   - Primary DNS server address
   - Default Gateway IP address
   - Administrator ID and Password
4. Log in to the web-based Management Console by browsing to https://x.x.x.x:8082 (replace x.x.x.x with the bridge IP address you assigned in the serial console).

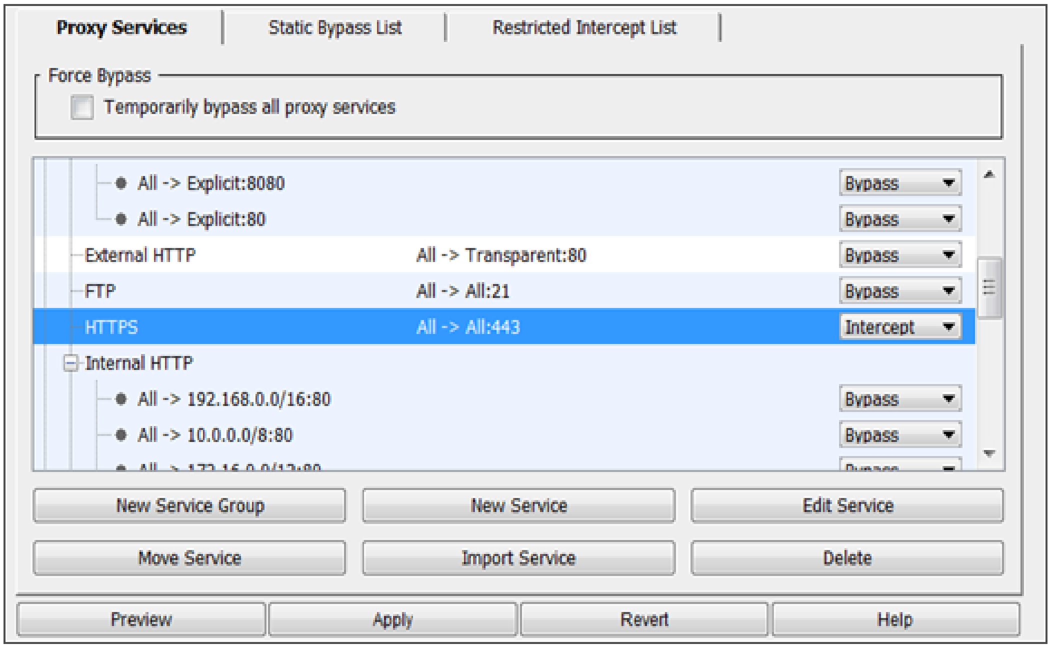
Next Step: Intercept User Traffic

Intercept User Traffic

After configuring how your ProxySG appliance receives user traffic, you need to configure proxy services. Without the appropriate services set to Intercept, that traffic will pass through the proxy without being subjected to policy. The most common ports to intercept are 80 (HTTP), 443 (HTTPS), and 554 (RTSP for flash streaming media).

Transparent Proxy Services

1. In the Management Console, select **Configuration > Services > Proxy Services**.
2. Under Predefined Service Groups, expand the **Standard** group. A list of services displays.
3. Locate the service you want to set to Intercept.
4. From the drop-down menu next to the service, select **Intercept**. In this example, the HTTPS service is set to Intercept.



Force Bypass

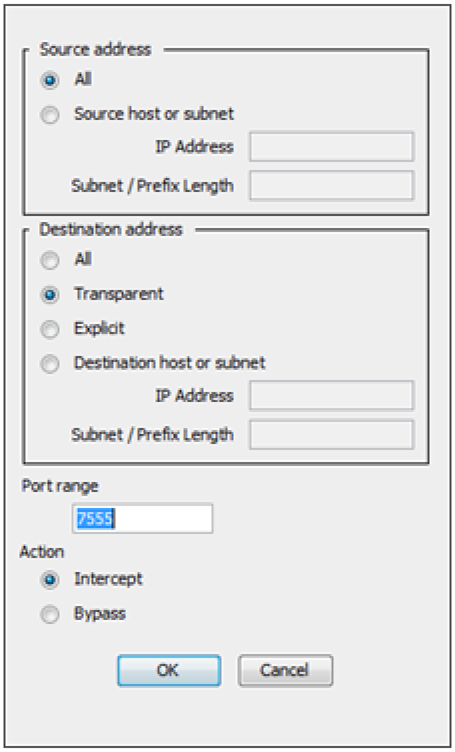
□ Temporarily bypass all proxy services

● All -> Explicit:8080		Bypass
● All -> Explicit:80		Bypass
External HTTP	All -> Transparent:80	Bypass
FTP	All -> All:21	Bypass
HTTPS	All -> All:443	Intercept
⊟ Internal HTTP		
● All -> 192.168.0.0/16:80		Bypass
● All -> 10.0.0.0/8:80		Bypass
● All -> 172.16.0.0/12:80		Bypass

5. Repeat steps 3 and 4 for each additional service you want to intercept.
6. (Optional) To intercept traffic types that are not predefined:
   a. Click **New Service**.
   b. Enter a name for the service and select the service group, under which the new service will be listed.
   c. Select a proxy type from the **Proxy** drop-down menu. This menu lists all of the types of traffic the ProxySG understands. If the type of traffic you are intercepting is not listed, select **TCP Tunnel**.

      Caution: Tunneled traffic can only be controlled based on the information contained in the TCP header of the request: client IP, destination IP, and source and destination ports.

   d. Click **Edit/Add Listeners**. The New Listener dialog displays.



Source address

● All

○ Source host or subnet

IP Address

Subnet / Prefix Length

Destination address

○ All

● Transparent

○ Explicit

○ Destination host or subnet

IP Address

Subnet / Prefix Length

Port range

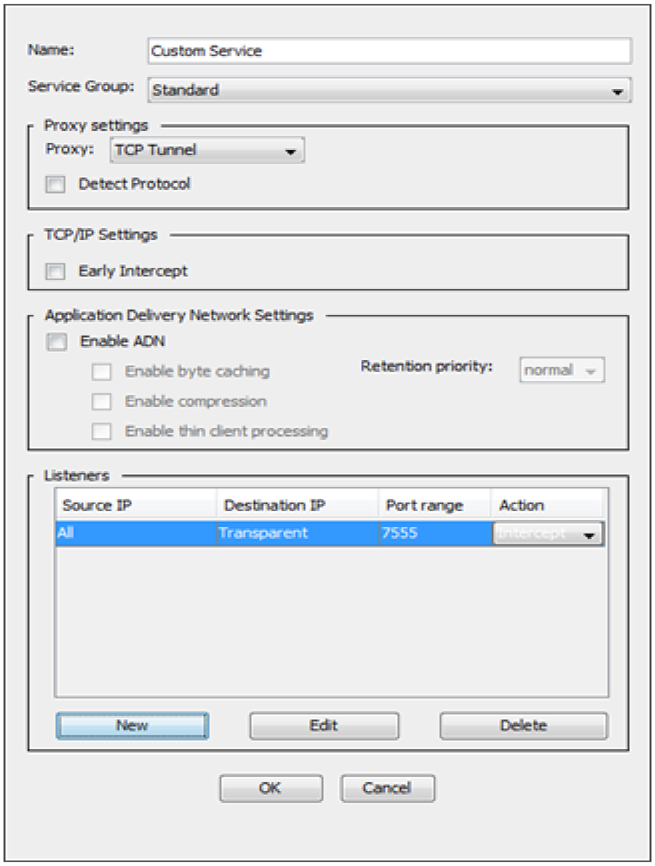
7555

Action

● Intercept

○ Bypass

e. In the **Port range** field, enter the port your application uses to communicate.
f. Ensure that the **Action** field is set to **Intercept** and click **OK**.
g. If enabled, uncheck **Enable ADN**.



Name: Custom Service

Service Group: Standard

Proxy settings

Proxy: TCP Tunnel

□ Detect Protocol

TCP/IP Settings

□ Early Intercept

Application Delivery Network Settings

□ Enable ADN

□ Enable byte caching

□ Enable compression

□ Enable thin client processing

Retention priority: normal

Listeners

Source IP	Destination IP	Port range	Action
All	Transparent	7555	Intercept

h. Click **OK** .

7. Click **Apply**. The appliance confirms your changes.

   Tip If your network has servers or devices that require a direct connection to the Internet, use the **Static Bypass List** to define the IP addresses for those servers or clients to be exempted from proxy service interception.

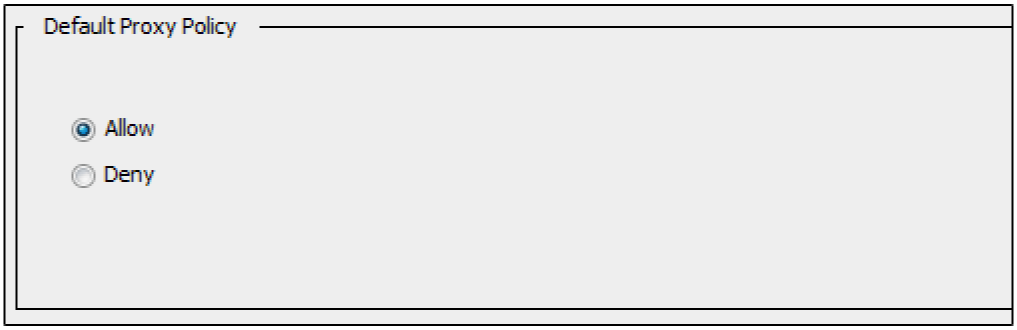
Next Step: Configure the Default Proxy Policy

Configure the Default Proxy Policy

Now that traffic is being directed to and intercepted by the appliance, it's time to consider how client requests will interact with policy. The first step is to set the default policy action. This controls traffic that does not match any rules in your visual or local policy.

1. In the web-based management console, browse to **Configuration > Policy > Policy Options**.
2. Set the **Default Proxy Policy** to **Allow** and click **Apply**.

   Setting the default proxy policy determines what the proxy will do with a request that doesn't match any rules you've configured in either the Visual Policy Manager or in CPL-based policy sets such as local and central. By default, the default proxy policy is set to deny. Though your scenario may differ, most administrators favor a default allow policy. Keep this in mind as you define policy in the VPM: if a URL or category is not explicitly denied, users will be able to get there.



Default Proxy Policy

● Allow

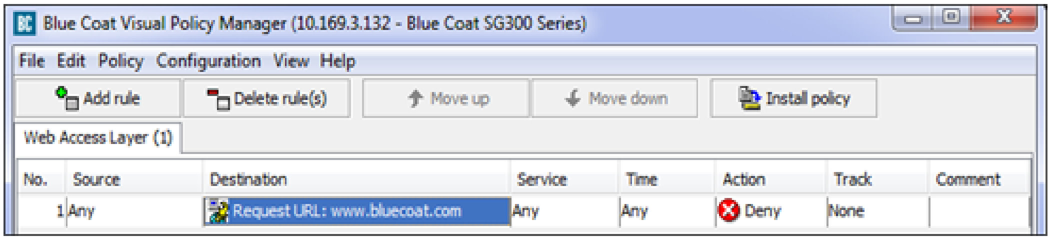
○ Deny

Next Step: Test Transparent Access

Test Transparent Access

To identify the sites and URL categories your users are permitted or denied access through the proxy, you need to create policy rules in the Visual Policy Manager (VPM). The proceeding sample policy will introduce you to working with the VPM and help to test transparent access to the Internet.

1. Select **Policy > Visual Policy Manager > Launch**. The Visual Policy Manager (VPM) displays.
2. In the VPM, select **Policy > Add Web Access Layer**. A new policy layer displays, with a single rule.
3. Right-click the **Destination** column and select **Set > New > Request URL**.
4. Enter a URL to use for testing, **www.bluecoat.com**. Click **Add**, **Close** and **OK**.
5. Note the action in this rule. By default, it is **DENY**. Click **Install Policy** to commit this rule to your configuration.



Blue Coat Visual Policy Manager (10.169.3.132 - Blue Coat SG300 Series)

No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	Request URL: www.bluecoat.com	Any	Any	Deny	None	

6. From a workstation in the network, browse to www.google.com. Access is granted.
7. From the same workstation, browse to www.bluecoat.com. A deny exception page displays.
8. (Optional) Configure logging to verify your testing results.

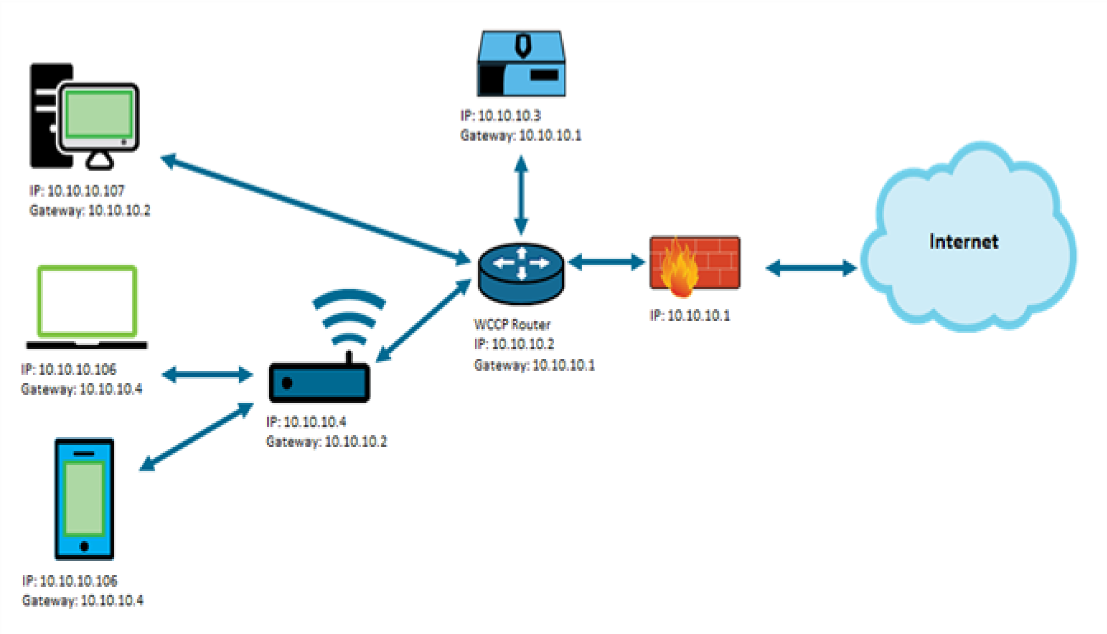
   Tip You can customize the deny pages users see when their requests match a deny rule. This type of page is called an *exception page*.

Configure WCCP Redirection

Web Cache Control Protocol (WCCP) is a Cisco protocol that directs user traffic to another device (in this case, a ProxySG appliance) for the purpose of caching and controlling content. WCCP configuration is available on many different switches, routers, and firewalls, made by Cisco or licensed by third-party companies. The ProxySG appliance supports

WCCP versions 1 and 2. WCCP version 2 allows traffic for any TCP port to be redirected to the proxy, while WCCP version 1 supports only port 80 (HTTP) redirection.

This configuration example is for a simple deployment consisting of one WCCP device and a single ProxySG appliance. WCCP supports multiple points of redirection and multiple ProxySG appliances and can load balance among them. For more information on WCCP redundancy and other advanced configuration options, see the Blue Coat WCCP Reference Guide.



1. Prepare a WCCP Device for Redirection.
2. Configure the ProxySG to Accept WCCP-Redirected Traffic.
3. Intercept User Traffic.
4. Configure the Default Proxy Policy .
5. Test Transparent Access.

Prepare a WCCP Device for Redirection

With WCCP, the ProxySG appliance works with a Cisco switch, router, or firewall to redirect traffic on its way out to the Internet. The simplified steps here will prepare your Cisco device for WCCP redirection. This sample configuration involves creating a redirect list (**wccp 99**) and an Access Control List (**access-list 101**) to direct all Internet-bound traffic to the ProxySG appliance.

1. Log on to your switch or router's command line interface (SSH or Telnet, as appropriate).
2. Identify the router interface that will be used to transmit data to and from the ProxySG appliance. This example uses interface **e0**.
3. Enter the following commands to configure WCCP and create an associated Access Control List, (ACL).

```
router(conf)# conf t
router(conf)# ip wccp 99 redirect-list 101
router(conf)# int e0
router(conf-if)# ip wccp 99 redirect out
router(conf)#access-list 101 permit ip host any
router(conf)#access-list 101 deny ip any any
```

Note: Remember the access list number you define here (101 in this example), as you will need to configure the ProxySG appliance with that information. The ProxySG refers to the access list as a *service group*.

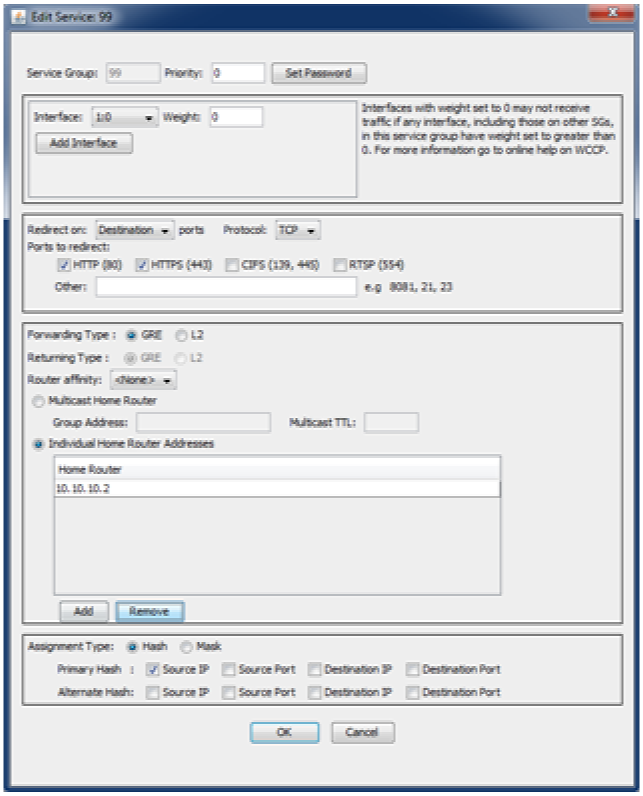
Next Step: Configure the ProxySG to Accept WCCP-Redirected Traffic

Configure the ProxySG to Accept WCCP-Redirected Traffic

This configuration example is for a simple deployment consisting of one WCCP device and one ProxySG appliance.

Configure your ProxySG appliance to accept redirected traffic from the WCCP device.

1. In the ProxySG Management Console, select **Configuration > Network > WCCP**.
2. Select **Enable WCCP**.
3. Select **New**. The **New Service** dialog displays.
4. Enter the **Service Group** you defined as an access list in the router configuration (101 in this example).
5. Select or define the TCP ports you want the ProxySG appliance to intercept and manage. This example redirects HTTP, HTTPS, and RTSP.
6. Select **Individual Home Router Addresses** and click **Add**. The New Home Router dialog displays.
7. Enter the IP address for the router that will perform WCCP redirection and click OK.



Edit Service: 99

Service Group: 99 Priority: 0 Set Password

Interface: 1:0 Weight: 0
Add Interface

Interfaces with weight set to 0 may not receive traffic if any interface, including those on other SGs, in this service group have weight set to greater than 0. For more information go to online help on WCCP.

Redirect on: Destination ports Protocol: TCP
Ports to redirect:
☑ HTTP (80) ☑ HTTPS (443) □ CIFS (139, 445) □ RTSP (554)
Other: e.g 8081, 21, 23

Forwarding Type : ● GRE ○ L2
Returning Type : ● GRE ○ L2
Router affinity: <None>
○ Multicast Home Router
Group Address: Multicast TTL:
● Individual Home Router Addresses

Home Router
10. 10. 10. 2

Add Remove

Assignment Type: ● Hash ○ Mask
Primary Hash : ☑ Source IP □ Source Port □ Destination IP □ Destination Port
Alternate Hash: □ Source IP □ Source Port □ Destination IP □ Destination Port

OK Cancel

8. Click **OK** and **Apply** to save the configuration.

When users request Internet resources, those requests will now be sent to the ProxySG appliance. In order to control that traffic, you will have to define the ports to intercept.

Next Step: Intercept User Traffic