ProxySG Reverse Proxy Deployment Guide

Version 7.1.x

Guide Revision: 9/3/2019

Symantec

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

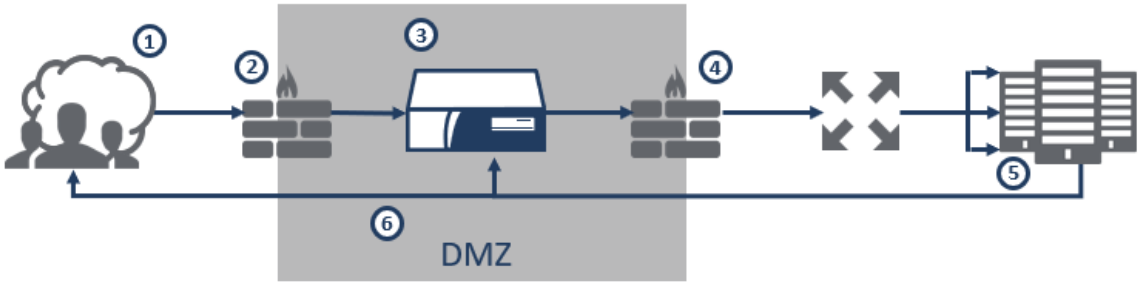
www.symantec.com

Tuesday, September 3, 2019

Table of Contents

About Reverse Proxy

A reverse proxy acts as a front-end to secure servers (such as Web, FTP, streaming, and more) and improves access performance. The most common type of reverse proxy is the Web Application Reverse Proxy (WARP). The following is a diagram of a typical reverse proxy deployment.



1. A user attempts to connect to a website via HTTP or HTTPS.
2. Traffic passes through the firewall to the ProxySG appliance. The ProxySG terminates the SSL connection to service the request.
3. The ProxySG appliance checks its internal cache for the user-requested content. If the content exists in the cache, the appliance immediately returns the response to the user. If the content is not in the cache, the appliance sends the request upstream, which might include sending the request off the appliance for DLP or CAS scanning, and, after verifying the request is safe, re-encrypting the request.
4. Traffic passes through the firewall and uses the selected load balancing method to route the request to the appropriate server. The firewall allows only the appliance to communicate with the web applications; therefore, potential attackers would need to bypass both the firewall and appliance, which obscures the internal URL structure of the content server. Restricting access to the content servers to only the appliance's IP address provides further security.
5. The ProxySG appliance retrieves the content from the web server and then stores the content in its cache so that when the content is next requested, the appliance can immediately retrieve it from the cache.
6. The ProxySG appliance delivers the content to the user.

Improve User Access with Reverse Proxy

In addition to securing your content and application servers, the reverse proxy further improves user access for the following:

User Authentication

The ProxySG appliance functions as an intermediary between users on the Internet and your content servers by challenging users to authenticate, or transparently checking for authentication credentials. The ProxySG appliance supports the following types of authentication:

- Local
- IWA
- LDAP
- RADIUS
- SAML

Real-Time Virus, Malware and Trojan Scanning

When deployed in conjunction with your ProxySG appliance, a ProxyAV appliance scans the data users upload to your content and application servers for most of today's Internet-borne threats.

SSL Encryption and Termination

The ProxySG appliance terminates HTTPS connections from users and forwards them to the server via HTTP, which reduces the resource load on your content and application servers. User connections remain secure as the appliance translates HTTP responses back into HTTPS.

Protocol Compliance

The ProxySG appliance ensures protocol compliance by detecting non-RFC-compliant attacks to limit exposure to vulnerabilities.

HTTP Compression

To further expedite delivery of web applications, the ProxySG appliance provides built-in gzip and Deflate. These compression services reduce the bandwidth required for serving content.

Content Acceleration

The ProxySG appliance quickly serves HTTP and HTTPS content via an optimized TCP stack. To accelerate content, the appliance uses the following methods:

- **Object pipelining:** The appliance retrieves several related elements at the same time.
- **Adaptive refresh:** The appliance regularly evaluates content that is stored in cache for freshness based on how frequently it is requested. With these advanced caching measures, the strain on your content servers is greatly reduced.

About Symantec Web Application Firewalls (WAF)

The Web Application Firewall (WAF) is an optional feature for reverse proxy configurations and requires an additional subscription. The WAF solves the challenges of securing your web-based applications, improving user experience, and reducing administrative overhead and performance. The Symantec WAF solution:

- Protects your web servers
- Accelerates web content
- Simplifies operation

For more information on the WAF, see the *SGOS Web Application Firewall Solutions Guide*.

If you also have Management Center, see *Management Center Web Application Firewall Policy Guide*.

Reverse Proxy Deployment Outline

Step	Solution Step	Document Reference
1	**Complete Pre-Deployment Requirements** ■ Obtain a license for your Reverse Proxy ■ Set up a public DNS record ■ Configure required ports and firewalls for forwarding ■ Install hardware and perform initial configuration ■ (Optional) Deploy a ProxyAV appliance to secure your Reverse Proxy	"Pre-Deployment Checklist" on page 11

Step	Solution Step	Document Reference
2	**Choose a deployment method:** **Deploy an Explicit Server Reverse Proxy** 1. (Optional) Configure a virtual IP on the ProxySG appliance 2. Define proxy services (HTTP or HTTPS) 3. Define forwarding hosts 4. Create an SSL Certificate Keyring or Keylist 5. Set up a basic policy **Deploy a Transparent Inline (Physically in-path) Reverse Proxy** 1. Create an SSL Certificate Keyring or Keylist 2. Create an HTTP Service 3. Create an HTTPS Service 4. Set up a basic policy **Deploy a Transparent Virtually in-path (Out-of-Path) Reverse Proxy** 1. Configure your WCCP Device to redirect traffic 2. Configure the ProxySG appliance to accept WCCP-redirected traffic 3. Intercept user traffic 4. Create an SSL Certificate Keyring or Keylist 5. Create an HTTP Service 6. Create an HTTPS Service 7. Set up a basic policy	"Deploy an Explicit Server Reverse Proxy" on page 13 "Deploy a Physically In-Path Transparent Reverse Proxy" on page 30 "Deploy a Virtually In-Path Transparent Reverse Proxy" on page 43
Optional	**Ensure Proper Traffic Redirection** ■ Determine the Origin IP of requests ■ Configure Two-Way URL Rewrite (TWURL) ■ Configure load balancing	"Redirect Traffic Destined for the OCS" on page 61

Step	Solution Step	Document Reference
Optional	**Configure the Reverse Proxy** ■ Configure user access to your web servers ◦ Configure authentication for users via the Management Console or CLI ■ Optimize reverse proxy performance ■ Configure the Web Application Firewall ■ Configure multi-tenant policy ■ View the reverse proxy log: bcreporterwarp_v1 access log	"Configure the Reverse Proxy" on page 66
Optional	**Maintain the Reverse Proxy** ■ Analyze log data - Splunk plug in	"Maintain the Reverse Proxy by Analyzing Log Data" on page 81

Pre-Deployment Checklist

Before you configure your ProxySG appliance to handle incoming traffic from the Internet, there are a few things that need to be set up:

- Public DNS Resolution

  To enable Internet users to reach your web server, set up a public DNS record:

  1. Identify the dedicated public IP address you'll use for this web server.
  2. Contact a DNS hosting service to have them translate your domain name, (www.example.com) to the dedicated public IP address.

- Firewall configuration and port forwarding

  To configure traffic forwarding:

  1. Ensure you have identified a dedicated public IP address.
  2. Ensure you have defined the IP address to accept traffic at your network's edge.
  3. Configure you firewall to forward traffic to the ProxySG appliance's internal IP address. This configuration is known as port forwarding or Virtual IP addressing, depending on the firewall vendor.

     > **Note:** For security, only forward the ports for which your web server serves data. Typically, that's TCP ports 80 and 443 for HTTP and HTTPS, and in some cases, FTP on TCP port 21.

     If your firewall provides an intrusion detection system (IDS) or intrusion prevention system (IPS) functionality, or inspects and controls the flow of data, be sure to consult the manufacturer's documentation for managing these security services when hosting websites.

- Initial setup of your ProxySG appliance

  Follow the steps to cable and configure your ProxySG appliance in the Quick Start Guide provided with your hardware. This information is also available on the Symantec Product Documentation site. To view the Quick Start Guide for your appliance, on the Symantec Product Documentation page, in the **Enter a Product Name** search field, type the model of your appliance, such as *SG-600*, and press Enter. From the dropdown, select the specific version, such as *SG-600-20*, and expand the **Deployment Guide** dropdown.

- Extra Symantec security: ProxyAV

  To secure your reverse proxy infrastructure, and the content that flows in and out of your network, Symantec recommends deploying a ProxyAV appliance.

See the *Integrating the ProxySG and ProxyAV Appliances Guide* for help with initial ProxyAV configuration tasks.

Deploy an Explicit Server Reverse Proxy

In an explicit server reverse proxy deployment, user requests resolve to the IP address of the ProxySG appliance. The appliance terminates the connection and opens its own connection to communicate with the OCS. For further information on the flow of traffic, see "About Reverse Proxy" on page 5.

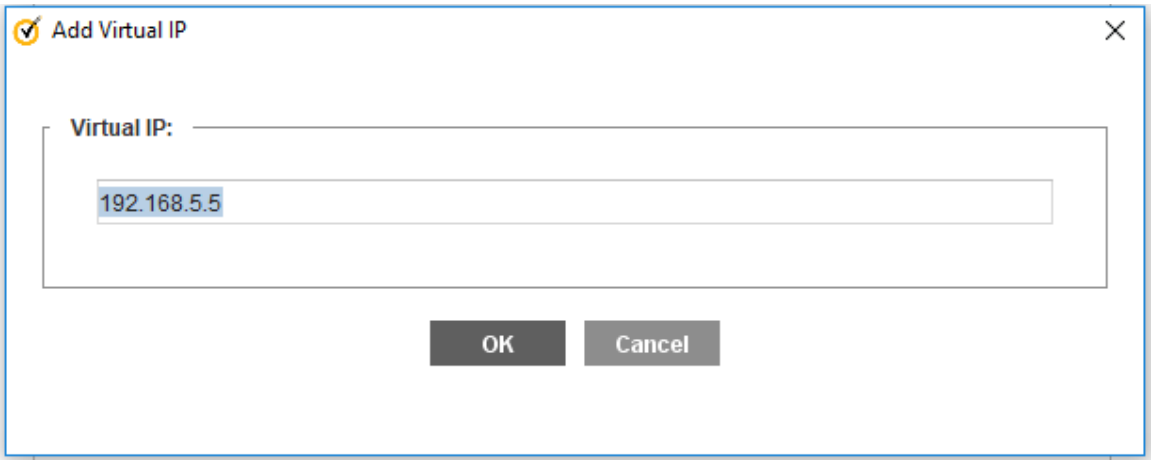
In an explicit server reverse proxy deployment, you will do the following:

1. "(Optional) Configure a Virtual IP Address" on the next page or "Create an SSL Certificate Keyring" on page 15.
2. "Create an HTTP Service for Your Reverse Proxy" on page 18 or "Create an HTTPS Service for Your Reverse Proxy" on page 21.
3. "Create a Forwarding Host" on page 24.
4. "Set Up Forwarding and Allow Policies" on page 26

(Optional) Configure a Virtual IP Address

Configure a virtual IP address (VIP) on the ProxySG appliance to take the place of a physical IP address. Using a VIP is useful if you are configuring your appliance to handle multiple reverse proxy-hosted websites on the same TCP port. If your deployment serves only a single host, VIP configuration and use is optional.

1. Log in to the Management Console.
2. Select **Configuration > Network > Advanced**.
3. In the **VIPs** tab, click **New**. The Add Virtual IP dialog appears.



4. Type the IP Address. In your initial planning stages, this is the IP address that will be used to handle incoming traffic from either your edge firewall or, if your ProxySG appliance is not protected by a firewall, the public address defined in the public DNS for your website.

> **Note:** The IP address must be unique and congruent with the other IP addresses defined on the appliance.

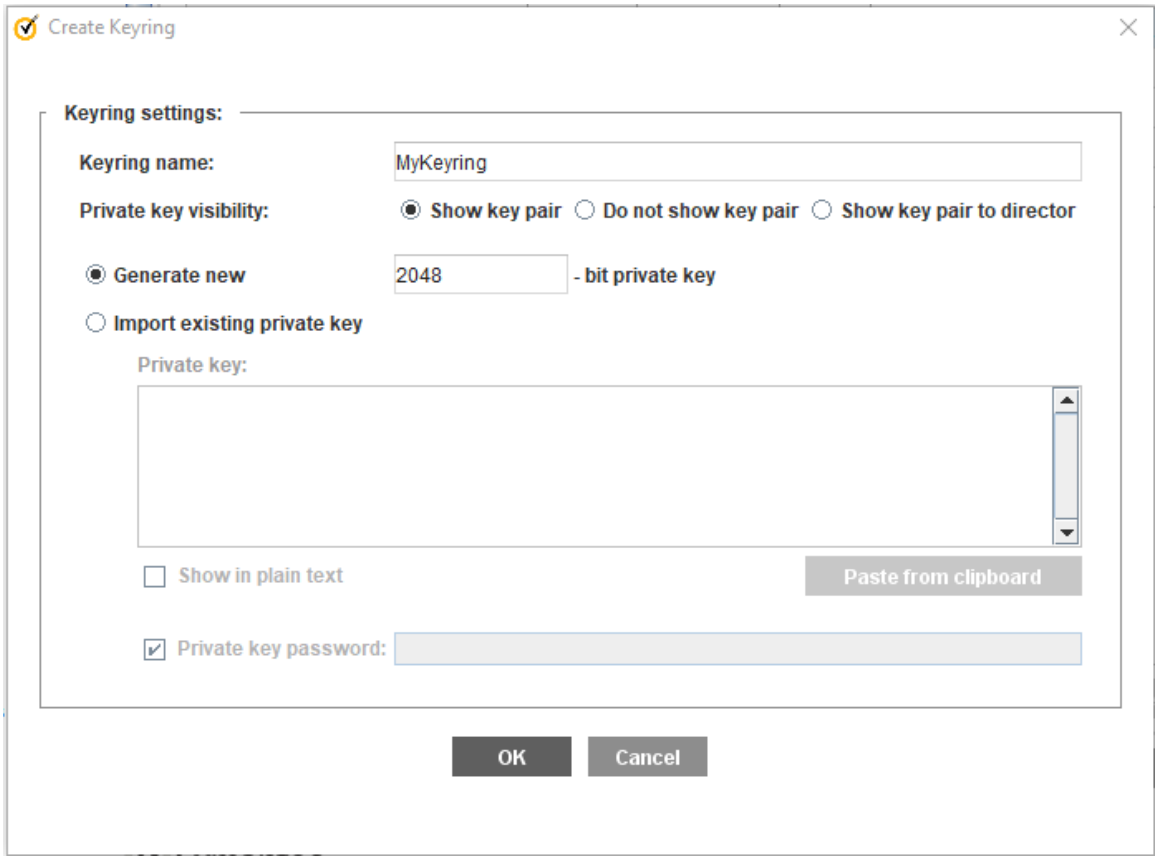
5. Click **OK** to create the VIP object.
6. Click **Apply** to save this object to your appliance's configuration.

Create an SSL Certificate Keyring

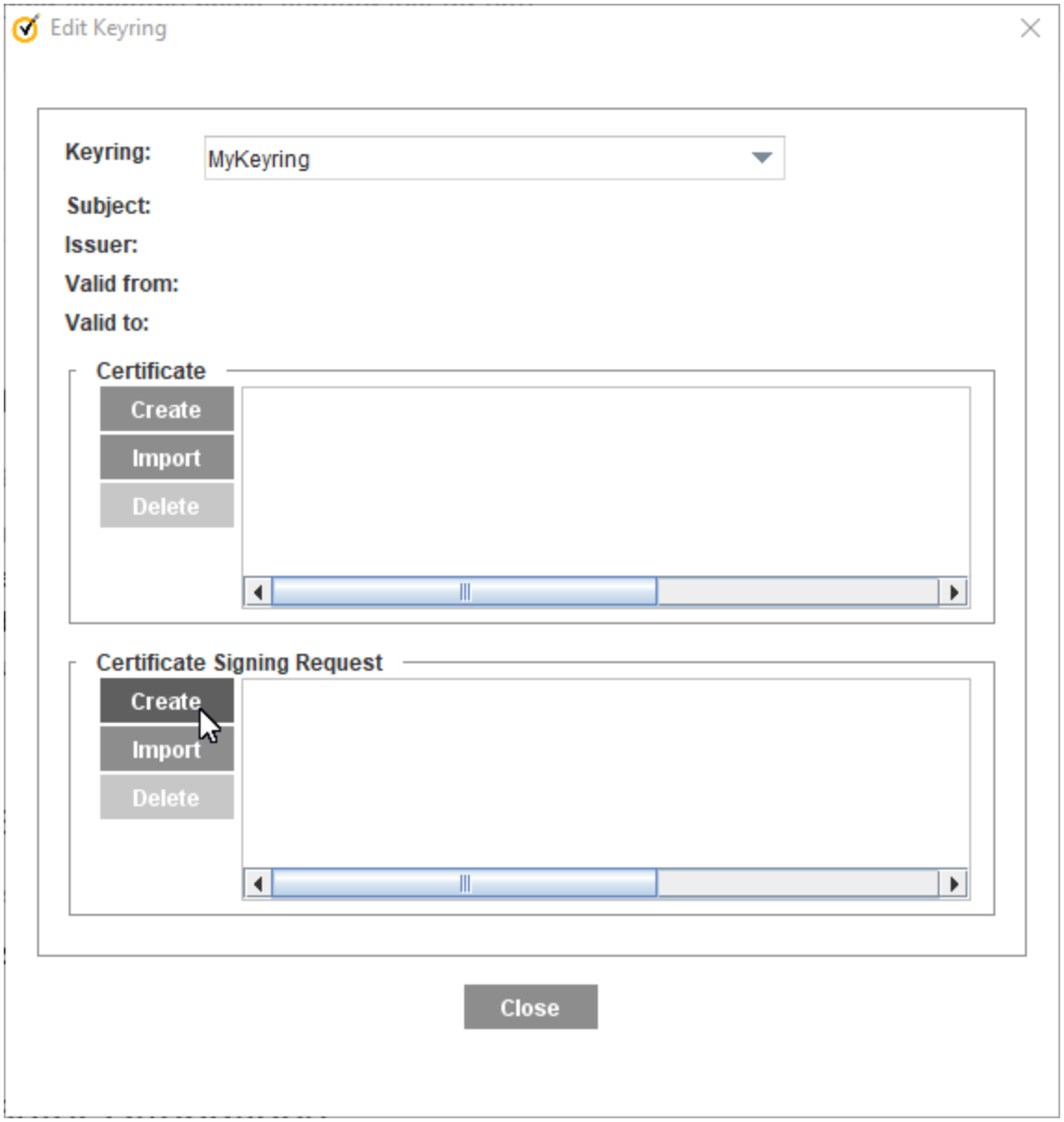
The ProxySG appliance uses a keyring to store certificates for HTTPS reverse proxy configurations. As users' HTTPS connections are terminated either before or on the appliance, you can choose whether traffic is sent using HTTP or HTTPS to your web servers.

To create an SSL certificate keyring:

1. Browse to the **Configuration > SSL > Keyrings** and click **Create**.

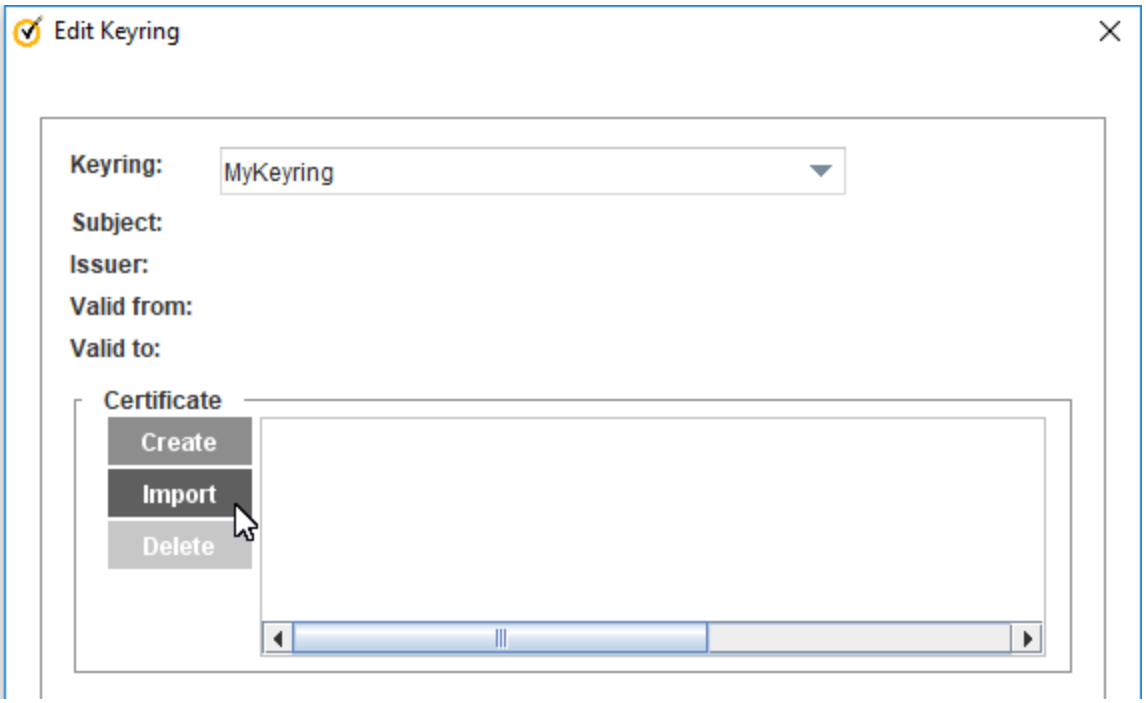


2. In the **Keyring name** field, type a name for the keyring.
3. Select **Show key pair** to permit backup and portability of the configuration.
4. In the **-bit private key** field, type the size for the key.
5. Click **OK** to create the keyring and commit the configuration to your appliance.
6. Select the keyring you created from the **Keyrings** list and click the **Edit** button.



7. In the **Certificate Signing Request** section, click **Create**. The Create Certificate Signing Request dialog displays.
8. Complete the form, paying close attention to the **Common Name** field. This should be a hostname or FQDN that resolves to the ProxySG appliance from outside of your protected network. This is the first step in ensuring that Internet-based browsers can trust the certificate the appliance presents. When you've completed the form, click **OK**, **Close**, and **Apply**.
9. Select the keyring and click **Edit** again. The Certificate Signing Request field contains a CSR in PKCS#10 format. Highlight the text from **-----BEGIN CERTIFICATE REQUEST-----** to **-----END CERTIFICATE REQUEST-----** and copy using **CTRL+C** (or on Apple systems, **the Apple key +C**) to copy the CSR to your system's clipboard.
10. Paste the CSR into a new text file on your local workstation and save the file with a .csr extension.

11. Send the CSR to be signed by a Certificate Authority (CA). The CA should provide you with a Root CA certificate as well as a server certificate. In some cases, an intermediate CA certificate is also provided.
12. Select the keyring and click **Edit** again.
13. In the **Certificate** section, click **Import**. The Import Certificate dialog opens. **Show screen.**

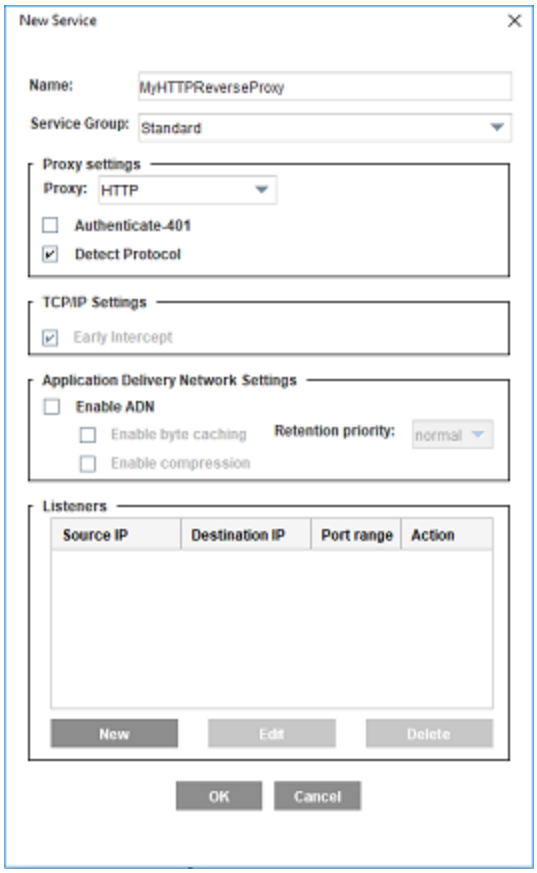


14. In the **Import Certificate** text box, paste the certificates in the order of first the server, then the intermediate, and then the CA certificate.
15. When all certificates have been entered into the text box, click **OK**, **Close**, and **Apply**.

Create an HTTP Service for Your Reverse Proxy

Configure an HTTP listener for your reverse proxy. This listener contains the IP address and TCP port that the ProxySG appliance uses to intercept traffic from the Internet or your edge firewall.

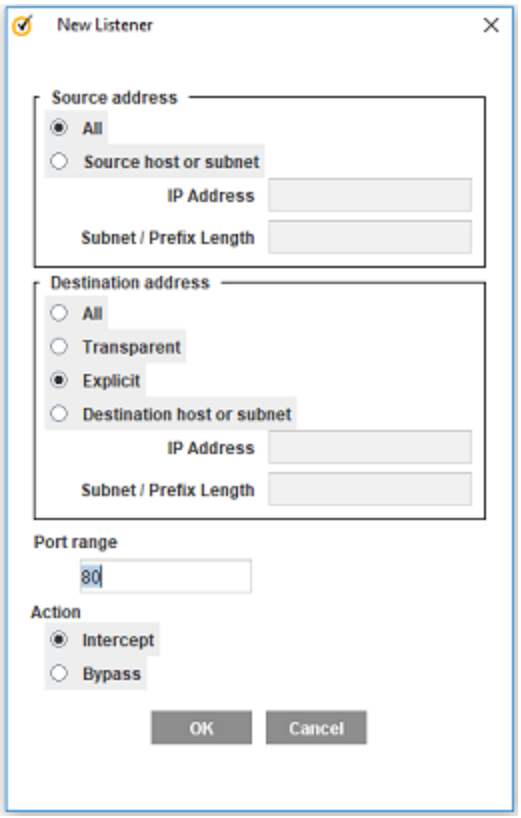
1. Log in to the Management Console.
2. Browse to **Configuration > Services > Proxy Services**.
3. Click the **New Service** button at the bottom of the page.



4. Type a name for the new service.
5. In the **Proxy** dropdown, select **HTTP** to handle simple HTTP-based websites. This proxy service type determines how the ProxySG appliance interprets and manages the traffic being passed through the service.
6. Enable **Detect Protocol**.
7. Ensure the **TCP/IP** parameter is set to **Early Intercept**. With early intercept, the ProxySG appliance returns a server acknowledgment back to the client and waits for the client acknowledgment, which completes the TCP 3-way

handshake before the appliance connects upstream to the server. For proxies that support object caching, the ProxySG appliance serves from the cache–a server connection is not necessary.

8. In the **Listeners** section, click **New**.



9. Unless your reverse proxy is deployed in a completely closed environment, Symantec recommends to leave the **Source Address** configuration at **All**. The **Source address** configuration is used to restrict the source of clients connecting through this service.

10. In the **Destination address** section, select **Explicit**.

    Optionally, you can select **Destination host or subnet** and, in **IP address**, type the address (either a physical address or one assigned to the appliance's interface or VIP address) the appliance is monitoring for connections that are relevant to this reverse proxy configuration. Use this option if the ProxySG appliance has multiple VIP addresses and you have configured different services for each or subsets of the IP addresses.

11. In **Port range**, define a port or a range or ports that the appliance will monitor for connections. If you plan to add multiple ports to your configuration, define only one port number per service object and repeat for as many ports as necessary.

12. Set the **Action** to **Intercept**.

13. Click **OK**.

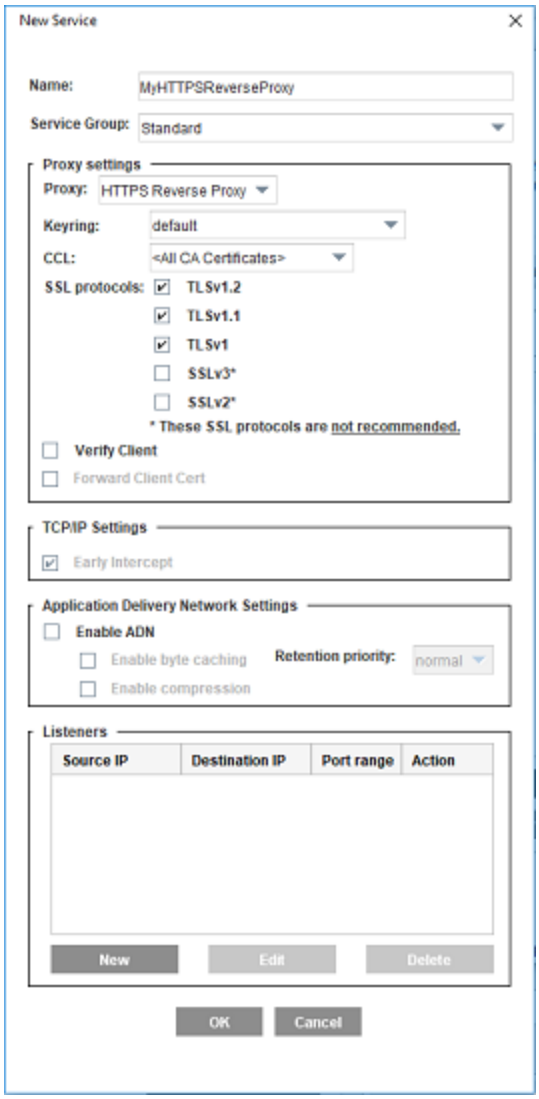
14. Click **OK**.

15. Click **Apply** to save the configuration.

Create an HTTPS Service for Your Reverse Proxy

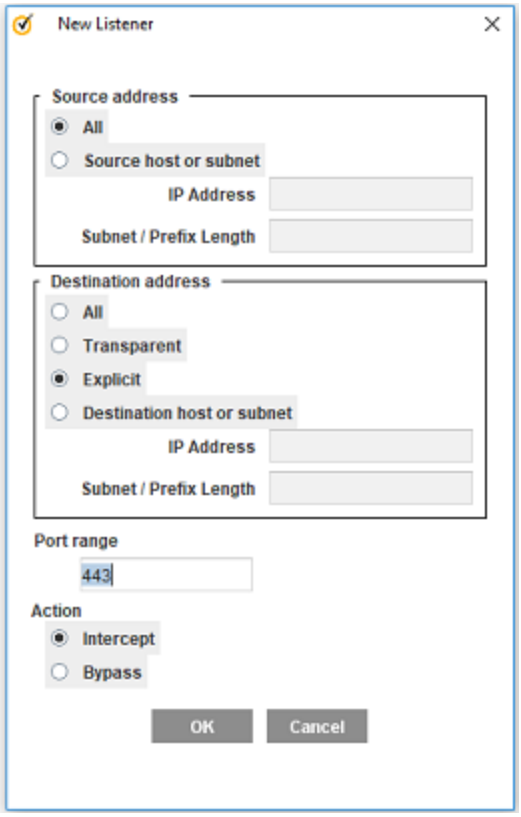
Configure a listener for your secure reverse proxy. This listener contains the IP address and TCP port that the ProxySG appliance uses to intercept traffic from the Internet or your edge firewall.

1. Log in to the Management Console.
2. Browse to the **Configuration > Services > Proxy Services**.
3. Click the **New Service** button at the bottom of the page.



4. Type a name for the new service.

5. In the **Proxy** drowdown, select **HTTPS Reverse Proxy** to handle secure HTTPS-based websites. This proxy service type determines how the ProxySG appliance interprets and manages the traffic being passed through the service.
6. Select the keyring you created for this configuration. If you have not created a keyring, "Create an SSL Certificate Keyring" on page 15.
7. In the **CCL** dropdown, select the CA Certificate List to be used to validate the certificate being presented to users. `<All CA Certificates>` is the default and suffices for most configurations.
8. Enable support for SSL protocols. SSLv3 and SSLv2 are not enabled by default as they are not recommended due to their insecure nature.
9. Disable ADN by deselecting the **Enable ADN** checkbox.
10. In the **Listeners** section, click **New**.



11. Unless your reverse proxy is deployed in a completely closed environment, Symantec recommends that you leave the **Source Address** configuration at **All**. The **Source Address** configuration is used to restrict the source of clients connecting through this service.
12. In the **Destination address** section, select **Explicit**.

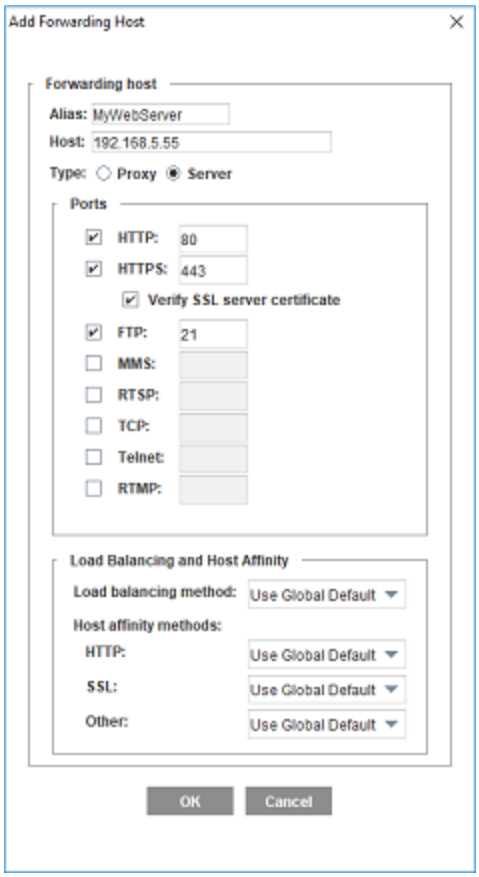
Optionally, you can select **Destination host or subnet** and, in **IP address**, type the address (either a physical address or one assigned to the appliance's interface or VIP address) the appliance is monitoring for connections that are relevant to this reverse proxy configuration. Use this option if the ProxySG appliance has multiple VIP addresses and you have configured different services for each or subsets of the IP addresses.

13. In **Port range**, define a port or a range or ports that the appliance will monitor for connections. For a standard HTTPS web server, type **443** as the port number. If you plan to add multiple ports to your configuration, define only one port number per service object and repeat for as many ports as necessary.
14. Set the **Action** to **Intercept**.
15. Click **OK**.
16. Click **OK**.
17. Click **Apply** to save the configuration.

Create a Forwarding Host

Create a new forwarding host to allow the ProxySG appliance to communicate with the server in your environment.

1. Log in to the Management Console.
2. Browse to the **Configuration tab > Forwarding > Forwarding Hosts**.
3. Under the **Forwarding Hosts** tab, click **New**.



4. In the **Alias** field, type a plain-text label for this forwarding host.

> **Note:** Spaces are not permitted in this field.

5. In the **Host** field, type the internal IP address of the server that hosts the content that is provided to users who pass through the ProxySG appliance.
6. For the **Type**, select **Server**.

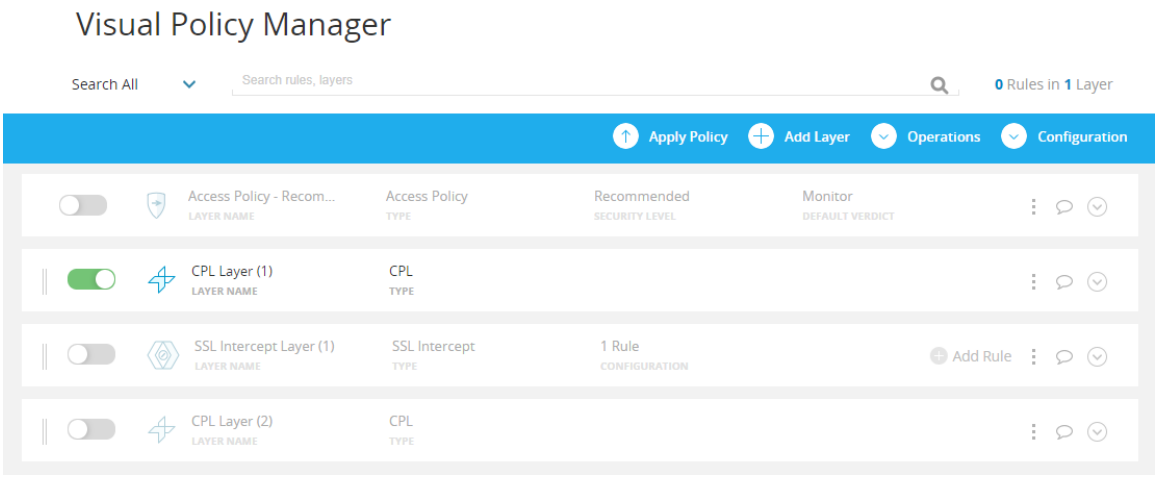
7. In the **Ports** section, enable the ports for any services you're hosting on this server (such as, HTTP, HTTPS, or FTP).
8. Click **OK** to save the forwarding host.
9. Click **Apply**.
10. (Optional) If you have multiple redundant content servers, "Configure Load Balancing on the ProxySG Appliance" on page 65 for the appliance.

Set Up Forwarding and Allow Policies

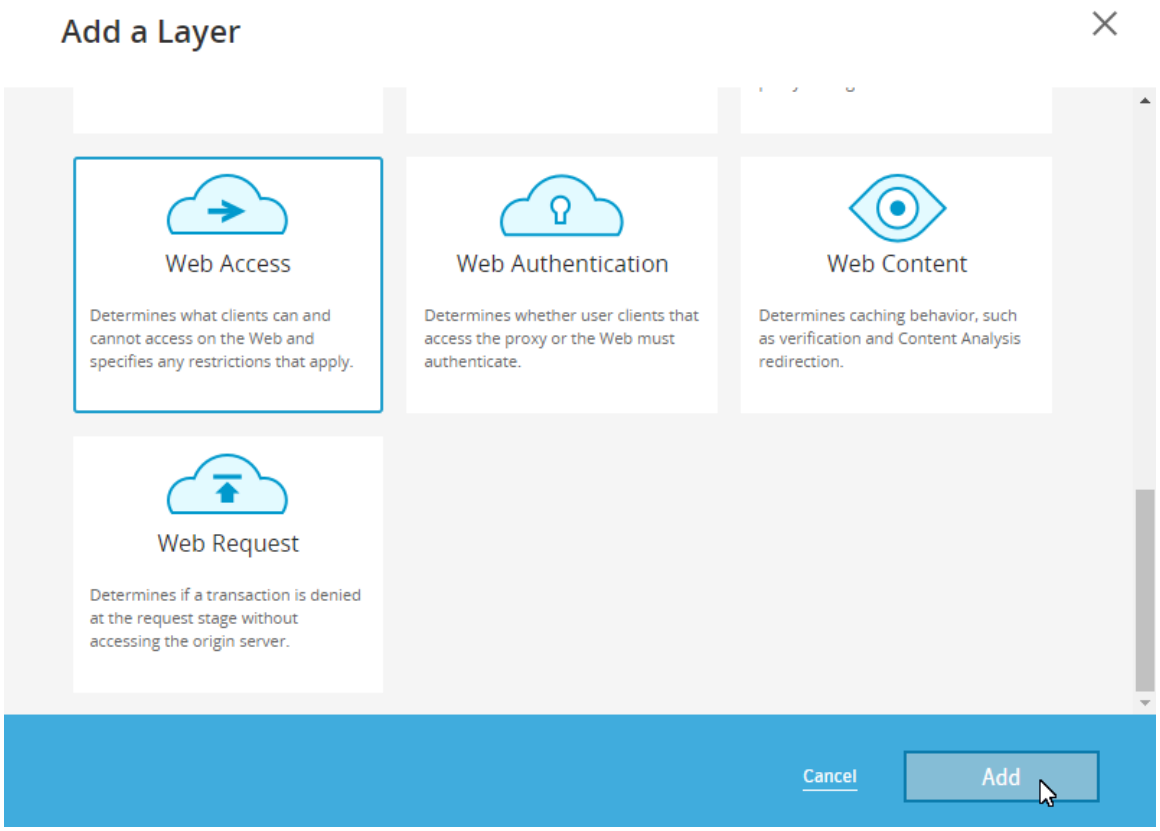
The ProxySG appliance uses policy to control how users on the Internet to access your content servers. Create policy to permit user access and to forward their requests to your back-end content servers.

> **Note:** Before you begin, select the portal profile. If you have not enabled the portal profile, see "Enable the Portal Profile" on page 29.

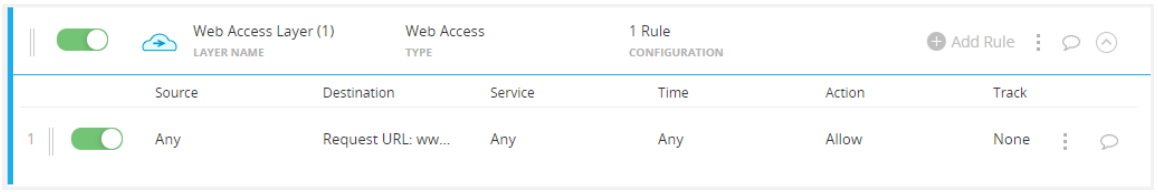
1. Log in to the Management Console.
2. Browse to **Configuration > Policy > Visual Policy Manager**.
3. Click **Launch VPM**.



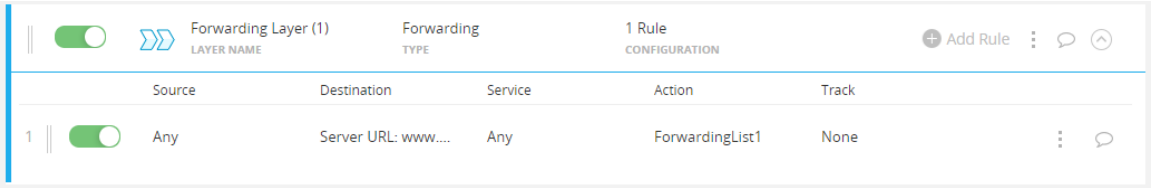
4. Click **Add a Layer**.
5. Select **Web Access** and click **Add**. **Show screen.**



6. Type a name for the layer and click **OK**. The new layer appears at the bottom of the list of layers.
7. Under **Destination**, click the cell and click **Set**.
8. Click **Add new object** and select **Request URL**.
9. Select **Simple Match**.
10. In the **URL** field, type the domain name users use to access the website the reverse proxy will be servicing.
11. Click **Apply**.
12. Click **Set**.
13. For your new Web Access Layer, under **Action**, click the cell and click **Allow**.



14. Click **Add a Layer**.
15. Select **Forwarding** and click **Add**.
16. Type a name for the layer and click **OK**. The new layer appears at the bottom of the list of layers.
17. Under **Destination**, click the cell and click **Set**.
18. Click **Add new object** and select **Server URL**.
19. In the **URL** field, type the domain name users use to access the website the reverse proxy will be servicing.
20. Click **Apply**.
21. Click **Set**.
22. For your new Forwarding Layer, under **Action**, click the cell and click **Set**.
23. Click **Add new object** and select **Select Forwarding**.
24. Type a name for the object.
25. In the **Available** list of forwarding hosts, select the forwarding host you previously created and move it to the **Selected - Ordered List**.
26. Click **Apply**.
27. Ensure the object you just created is selected and click **Set**.



28. Click **Apply policy** and click **OK**.

Next Step: You have completed the basic steps for deploying your reverse proxy. To further improve the effectiveness of your reverse proxy, you can "Enable the Portal Profile" on page 42, "Redirect Traffic Destined for the OCS" on page 61, "Configure the Reverse Proxy" on page 66, or "Maintain the Reverse Proxy by Analyzing Log Data" on page 81.

Enable the Portal Profile

The HTTP Proxy portal profile acts as a server accelerator for the reverse proxy, and is used for web hosting. A server accelerator services requests meant for an OCS, as if it is the OCS itself.

To select the Portal Profile, go to **Management Console > Configuration > Proxy Settings > HTTP Proxy > Acceleration Profile**, and click **Use Portal Profile**.

Deploy a Physically In-Path Transparent Reverse Proxy

In a physically in-path transparent reverse proxy deployment, user requests resolve to the IP address of an appliance, such as a router, load balancer, switch, and so on. The appliance then terminates the connection and opens its own connection which passes through the ProxySG appliance before reaching the OCS.

This deployment method places the ProxySG appliance in the physical network path, between users and the OCS, 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 OCS.

In a physically in-path transparent reverse proxy deployment, you will do the following:

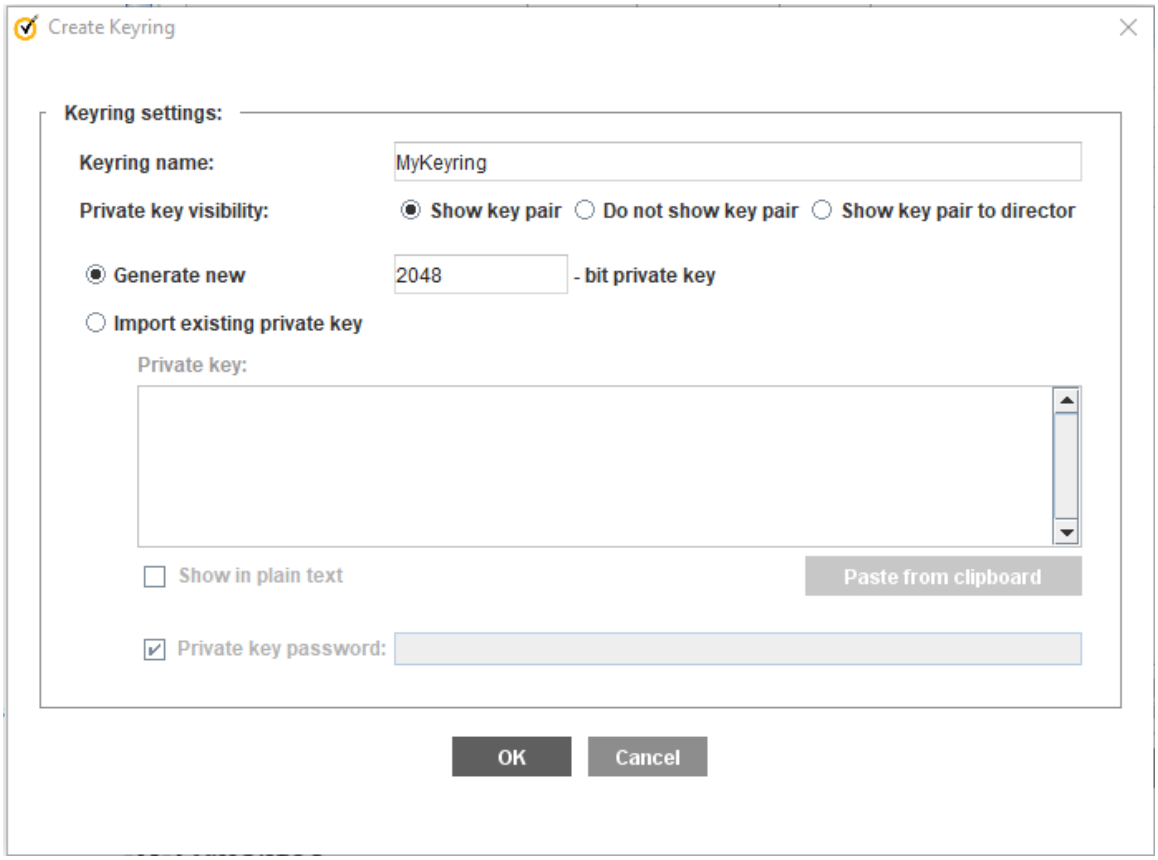
1. "Create an SSL Certificate Keyring" on the next page.
2. "Create an HTTP Service for Your Reverse Proxy" on page 34.
3. "Create an HTTPS Service for Your Reverse Proxy" on page 36
4. "Set Up an Allow Policy" on page 39

Create an SSL Certificate Keyring

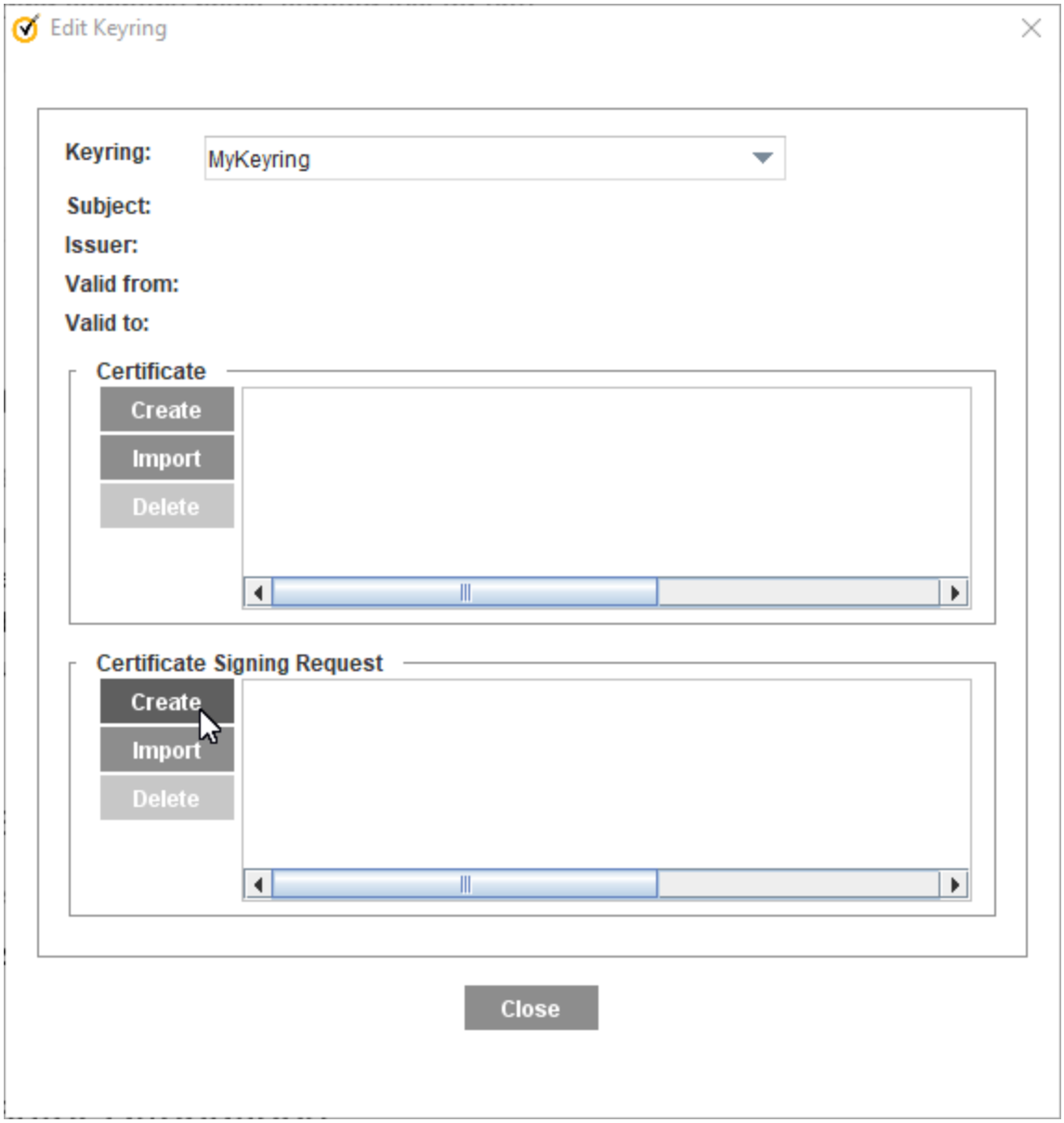
The ProxySG appliance uses a keyring to store certificates for HTTPS reverse proxy configurations. As users' HTTPS connections are terminated either before or on the appliance, you can choose whether traffic is sent using HTTP or HTTPS to your web servers.

To create an SSL certificate keyring:

1. Browse to the **Configuration > SSL > Keyrings** and click **Create**.

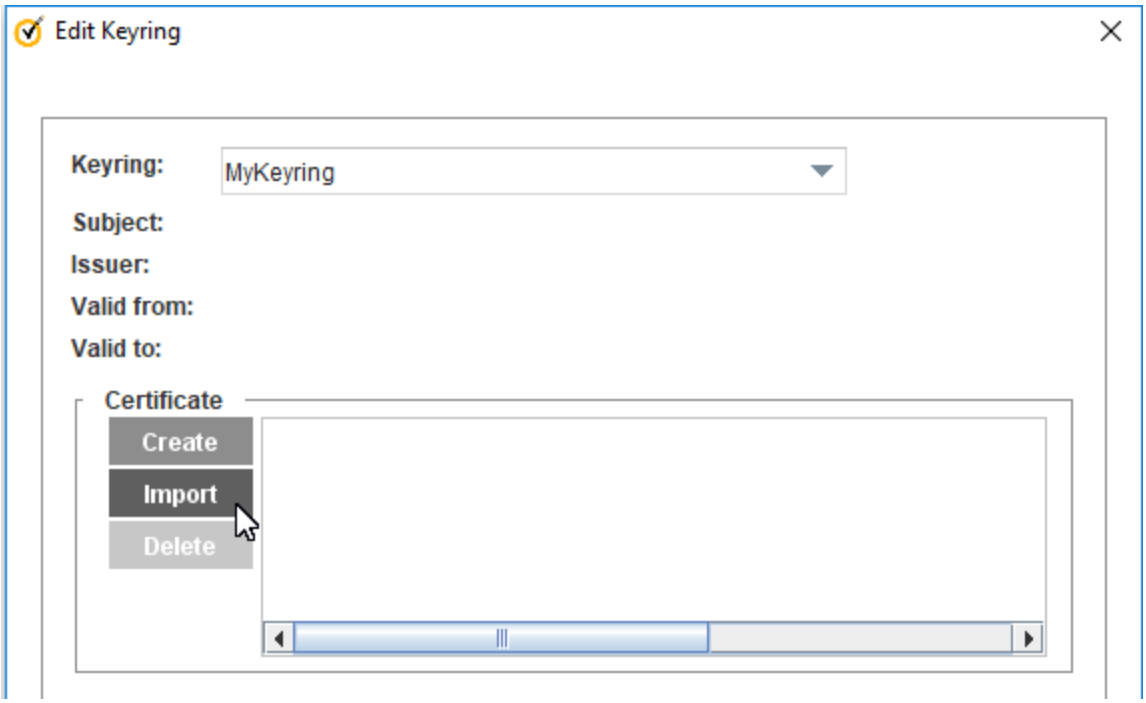


2. In the **Keyring name** field, type a name for the keyring.
3. Select **Show key pair** to permit backup and portability of the configuration.
4. In the **-bit private key** field, type the size for the key.
5. Click **OK** to create the keyring and commit the configuration to your appliance.
6. Select the keyring you created from the **Keyrings** list and click the **Edit** button.



7. In the **Certificate Signing Request** section, click **Create**. The Create Certificate Signing Request dialog displays.
8. Complete the form, paying close attention to the **Common Name** field. This should be a hostname or FQDN that resolves to the ProxySG appliance from outside of your protected network. This is the first step in ensuring that Internet-based browsers can trust the certificate the appliance presents. When you've completed the form, click **OK**, **Close**, and **Apply**.
9. Select the keyring and click **Edit** again. The Certificate Signing Request field contains a CSR in PKCS#10 format. Highlight the text from **-----BEGIN CERTIFICATE REQUEST-----** to **-----END CERTIFICATE REQUEST-----** and copy using **CTRL+C** (or on Apple systems, **the Apple key +C**) to copy the CSR to your system's clipboard.
10. Paste the CSR into a new text file on your local workstation and save the file with a .csr extension.

11. Send the CSR to be signed by a Certificate Authority (CA). The CA should provide you with a Root CA certificate as well as a server certificate. In some cases, an intermediate CA certificate is also provided.
12. Select the keyring and click **Edit** again.
13. In the **Certificate** section, click **Import**. The Import Certificate dialog opens. **Show screen.**

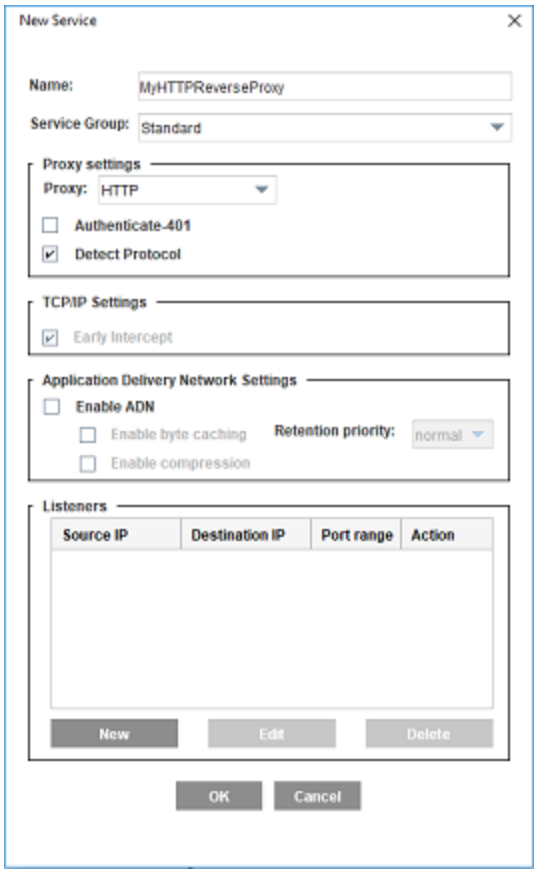


14. In the **Import Certificate** text box, paste the certificates in the order of first the server, then the intermediate, and then the CA certificate.
15. When all certificates have been entered into the text box, click **OK**, **Close**, and **Apply**.

Create an HTTP Service for Your Reverse Proxy

Configure an HTTP listener for your reverse proxy. This listener contains the IP address and TCP port that the ProxySG appliance uses to intercept traffic from the Internet or your edge firewall.

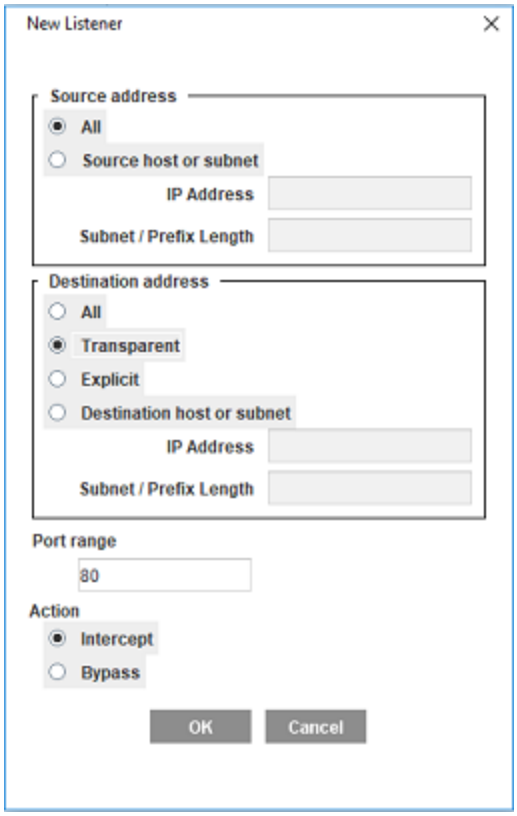
1. Log in to the Management Console.
2. Browse to **Configuration > Services > Proxy Services**.
3. Click the **New Service** button at the bottom of the page.



4. Type a name for the new service.
5. In the **Proxy** dropdown, select **HTTP** to handle simple HTTP-based websites. This proxy service type determines how the ProxySG appliance interprets and manages the traffic being passed through the service.
6. Enable **Detect Protocol**.
7. Ensure the **TCP/IP** parameter is set to **Early Intercept**. With early intercept, the ProxySG appliance returns a server acknowledgment back to the client and waits for the client acknowledgment, which completes the TCP 3-way

handshake before the appliance connects upstream to the server. For proxies that support object caching, the ProxySG appliance serves from the cache–a server connection is not necessary.

8. In the **Listeners** section, click **New**.

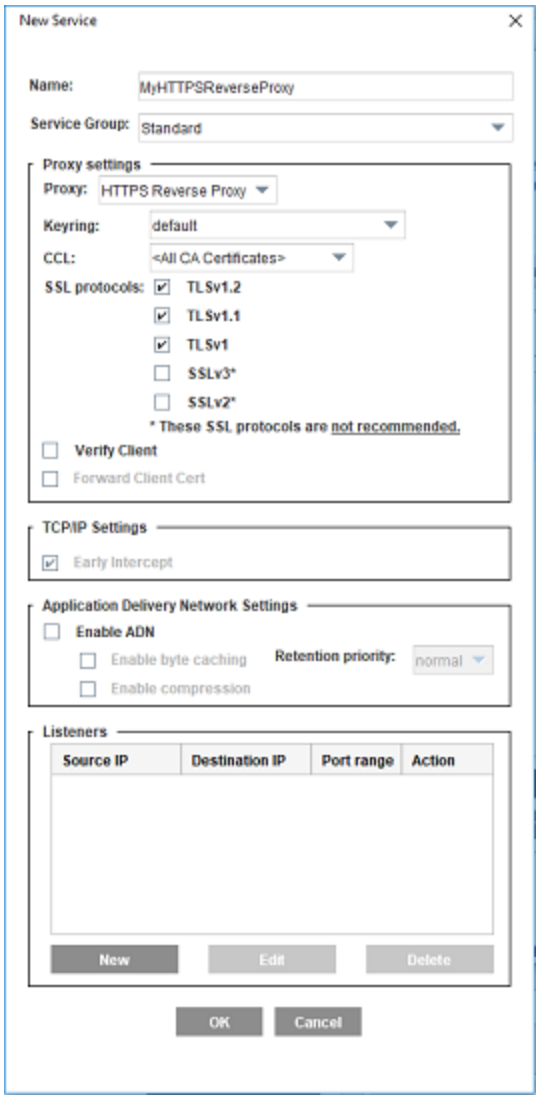


9. Unless your reverse proxy is deployed in a completely closed environment, Symantec recommends to leave the **Source Address** configuration at **All**. The **Source address** configuration is used to restrict the source of clients connecting through this service.
10. In the **Destination Address**, select **Transparent**.
11. In **Port range**, define a port or a range or ports that the appliance will monitor for connections. If you plan to add multiple ports to your configuration, define only one port number per service object and repeat for as many ports as necessary.
12. Set the **Action** to **Intercept**.
13. Click **OK**.
14. Click **OK**.
15. Click **Apply** to save the configuration.

Create an HTTPS Service for Your Reverse Proxy

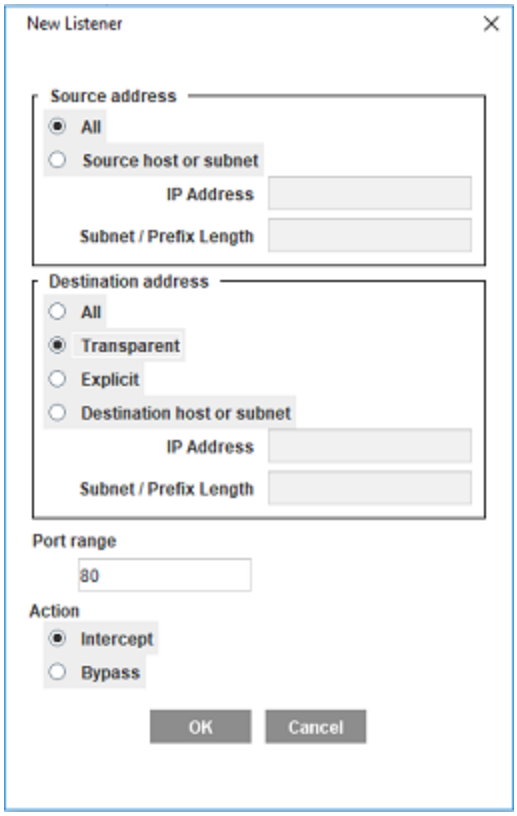
Configure a listener for your secure reverse proxy. This listener contains the IP address and TCP port that the ProxySG appliance uses to intercept traffic from the Internet or your edge firewall.

1. Log in to the Management Console.
2. Browse to the **Configuration > Services > Proxy Services**.
3. Click the **New Service** button at the bottom of the page.



4. Type a name for the new service.

5. In the **Proxy** drowdown, select **HTTPS Reverse Proxy** to handle secure HTTPS-based websites. This proxy service type determines how the ProxySG appliance interprets and manages the traffic being passed through the service.
6. Select the keyring you created for this configuration. If you have not created a keyring, "Create an SSL Certificate Keyring" on page 15.
7. In the **CCL** dropdown, select the CA Certificate List to be used to validate the certificate being presented to users. `<All CA Certificates>` is the default and suffices for most configurations.
8. Enable support for SSL protocols. SSLv3 and SSLv2 are not enabled by default as they are not recommended due to their insecure nature.
9. Disable ADN by deselecting the **Enable ADN** checkbox.
10. In the **Listeners** section, click **New**.



11. Unless your reverse proxy is deployed in a completely closed environment, Symantec recommends that you leave the **Source Address** configuration at **All**. The **Source Address** configuration is used to restrict the source of clients connecting through this service.
12. In the **Destination Address**, select **Transparent**.

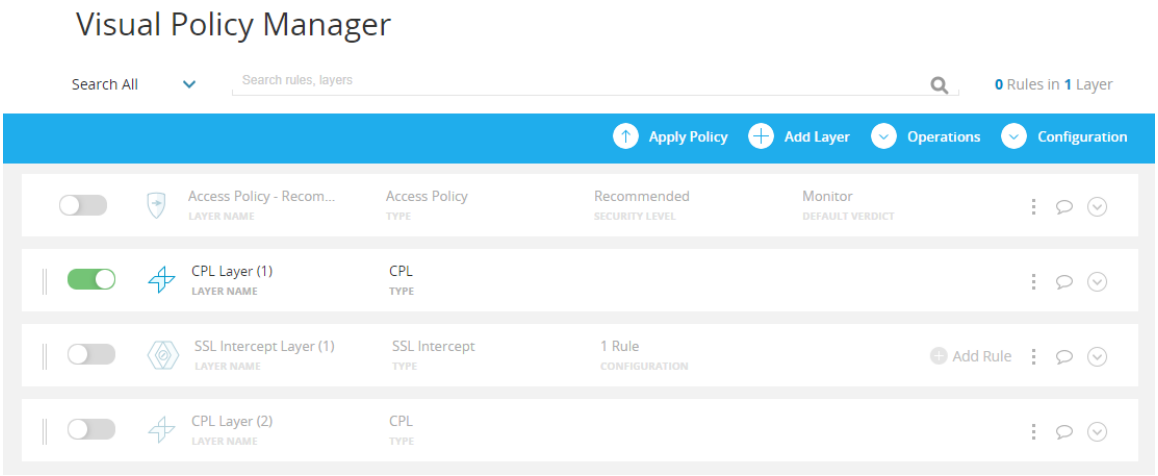
13. In **Port range**, define a port or a range or ports that the appliance will monitor for connections. For a standard HTTPS web server, type **443** as the port number. If you plan to add multiple ports to your configuration, define only one port number per service object and repeat for as many ports as necessary.
14. Set the **Action** to **Intercept**.
15. Click **OK**.
16. Click **OK**.
17. Click **Apply** to save the configuration.

Set Up an Allow Policy

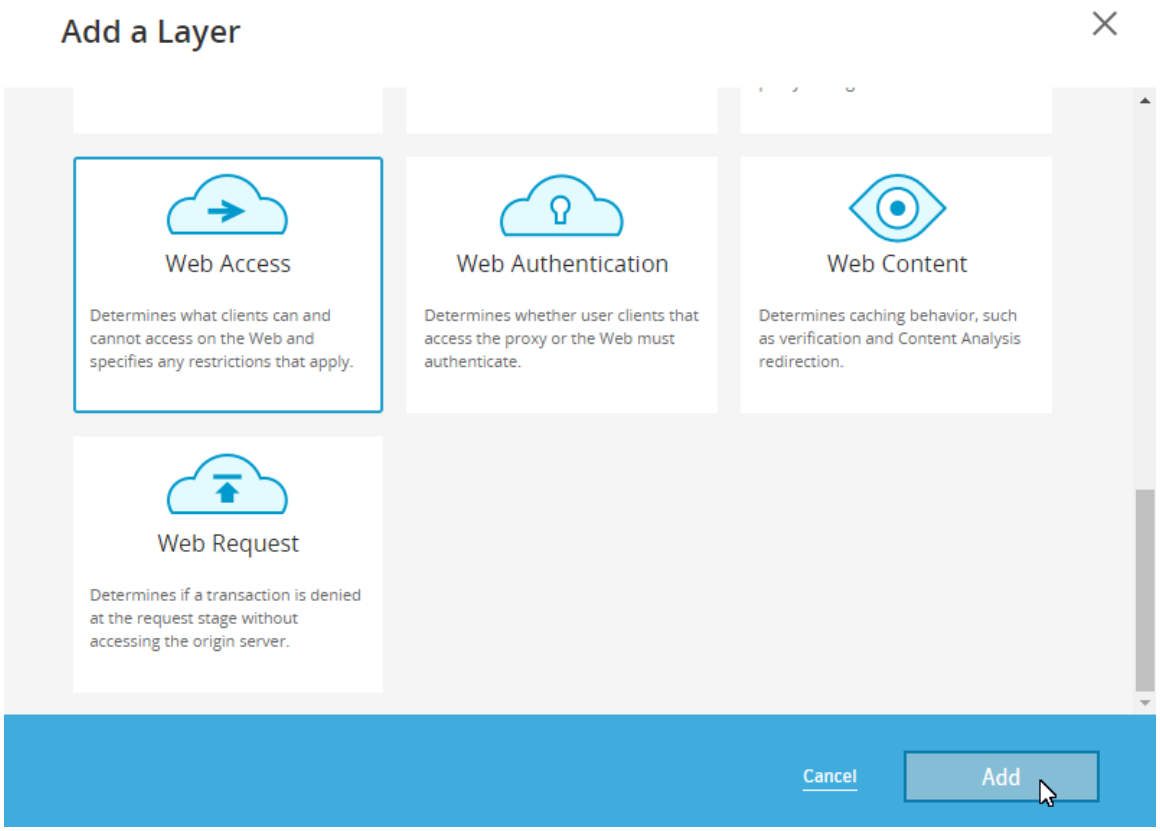
The ProxySG appliance uses policy to control how users on the Internet to access your content servers. Create policy to permit user access to your back-end content servers.

> **Note:** Before you begin, select the portal profile. If you have not enabled the portal profile, see "Enable the Portal Profile" on page 29.

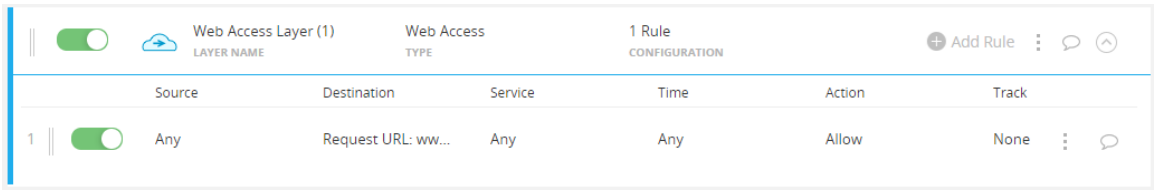
1. Log in to the Management Console.
2. Browse to **Configuration > Policy > Visual Policy Manager**.
3. Click **Launch VPM**.



4. Click **Add a Layer**.
5. Select **Web Access** and click **Add**. **Show screen.**



6. Type a name for the layer and click **OK**. The new layer appears at the bottom of the list of layers.
7. Under **Destination**, click the cell and click **Set**.
8. Click **Add new object** and select **Request URL**.
9. Select **Simple Match**.
10. In the **URL** field, type the domain name users use to access the website the reverse proxy will be servicing.
11. Click **Apply**.
12. Click **Set**.
13. For your new Web Access Layer, under **Action**, click the cell and click **Allow**.



14. Click **Apply policy** and click **OK**.

Next Step: You have completed the basic steps for deploying your reverse proxy. To further improve the effectiveness of your reverse proxy, you can "Enable the Portal Profile" on the facing page, "Redirect Traffic Destined for the OCS" on page 61, "Configure the Reverse Proxy" on page 66, or "Maintain the Reverse Proxy by Analyzing Log Data" on page 81.

Enable the Portal Profile

The HTTP Proxy portal profile acts as a server accelerator for the reverse proxy, and is used for web hosting. A server accelerator services requests meant for an OCS, as if it is the OCS itself.

To select the Portal Profile, go to **Management Console > Configuration > Proxy Settings > HTTP Proxy > Acceleration Profile**, and click **Use Portal Profile**.

Deploy a Virtually In-Path Transparent Reverse Proxy

In a virtually in-path transparent reverse proxy deployment, user requests resolve to the IP address of an appliance, such as a router, load balancer, switch, and so on. The appliance then terminates the connection and opens its own connection which is rerouted via Web Cache Control Protocol (WCCP) to the ProxySG appliance before reaching the OCS.

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 appliance for processing and policy evaluation. WCCP provides options for balancing load among several ProxySG appliance and is fault tolerant, sending traffic to the Internet directly, should the ProxySG appliance be unable to handle requests.

In a virtually in-path transparent reverse proxy deployment, you will do the following:

1. "Configure a WCCP Device for Redirection" on the next page.
2. "Configure the ProxySG appliance to Accept WCCP-Redirected Traffic" on page 45
3. "Intercept User Traffic" on page 47.
4. "Create an SSL Certificate Keyring" on page 49.
5. "Create an HTTP Service for Your Reverse Proxy" on page 52.
6. "Create an HTTPS Service for Your Reverse Proxy" on page 54.
7. "Set Up an Allow Policy" on page 57.

Configure a WCCP Device for Redirection

If your configuration requires a device, such as a Cisco switch, router, or firewall, to forward and receive traffic to and from the ProxySG appliance, configure that device to redirect traffic via Web Cache Control Protocol (WCCP) to the appliance.

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.

To prepare your device for redirection:

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. Type 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 appliance refers to the access list as a *service group*.

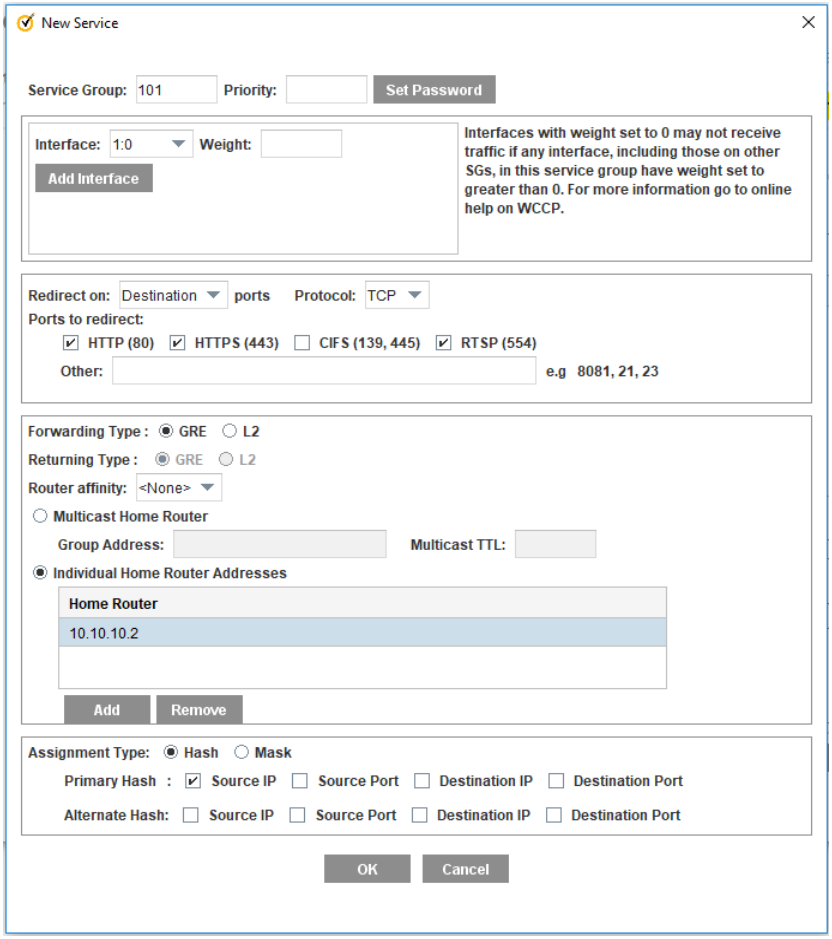
Configure the ProxySG appliance to Accept WCCP-Redirected Traffic

If your configuration requires a device, such as a Cisco switch, router, or firewall, to forward and receive traffic to and from the ProxySG appliance, configure the ProxySG appliance to redirect traffic via Web Cache Control Protocol (WCCP) to the device.

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

To configure your ProxySG appliance to accept redirected traffic from the WCCP device:

1. In the Management Console, select **Configuration > Network > WCCP**.
2. Select the **Enable WCCP** checkbox.
3. Click **New**. The New Service dialog displays.
4. Type 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. Type the IP address for the router that performs WCCP redirection and click **OK**.



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

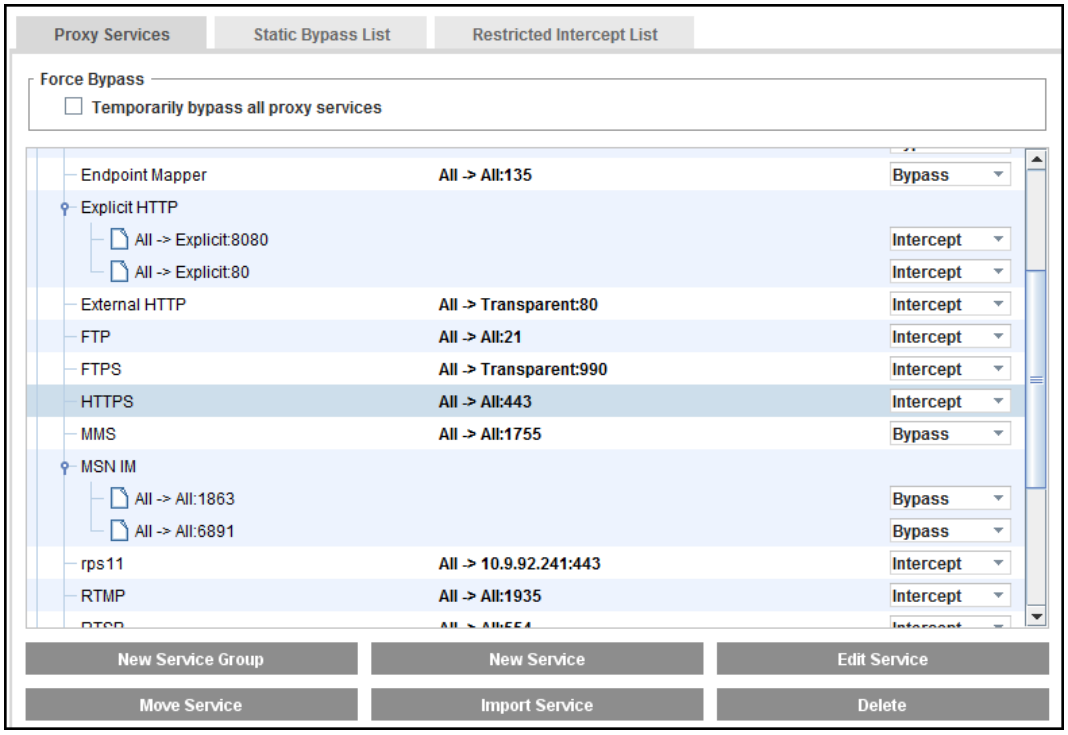
When users request Internet resources, those requests are now sent to the ProxySG appliance. To control those requests, define the ports to intercept.

Intercept User Traffic

Configure proxy services to intercept and subject traffic to policy. The most common ports to intercept are 80 (HTTP), 443 (HTTPS), and 554 (RTSP for flash streaming media). For more information on ports, see *Required ports, protocols, and services for ProxySGappliance*.

To configure the proxy services to intercept user traffic:

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**.



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**. The New Service dialog opens.
    b. Type 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 appliance 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. In the Listeners section, click either **Edit** or **New**. The Edit Listener or New Listener dialog displays.

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, deselect **Enable ADN**

h. Click **OK**.

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

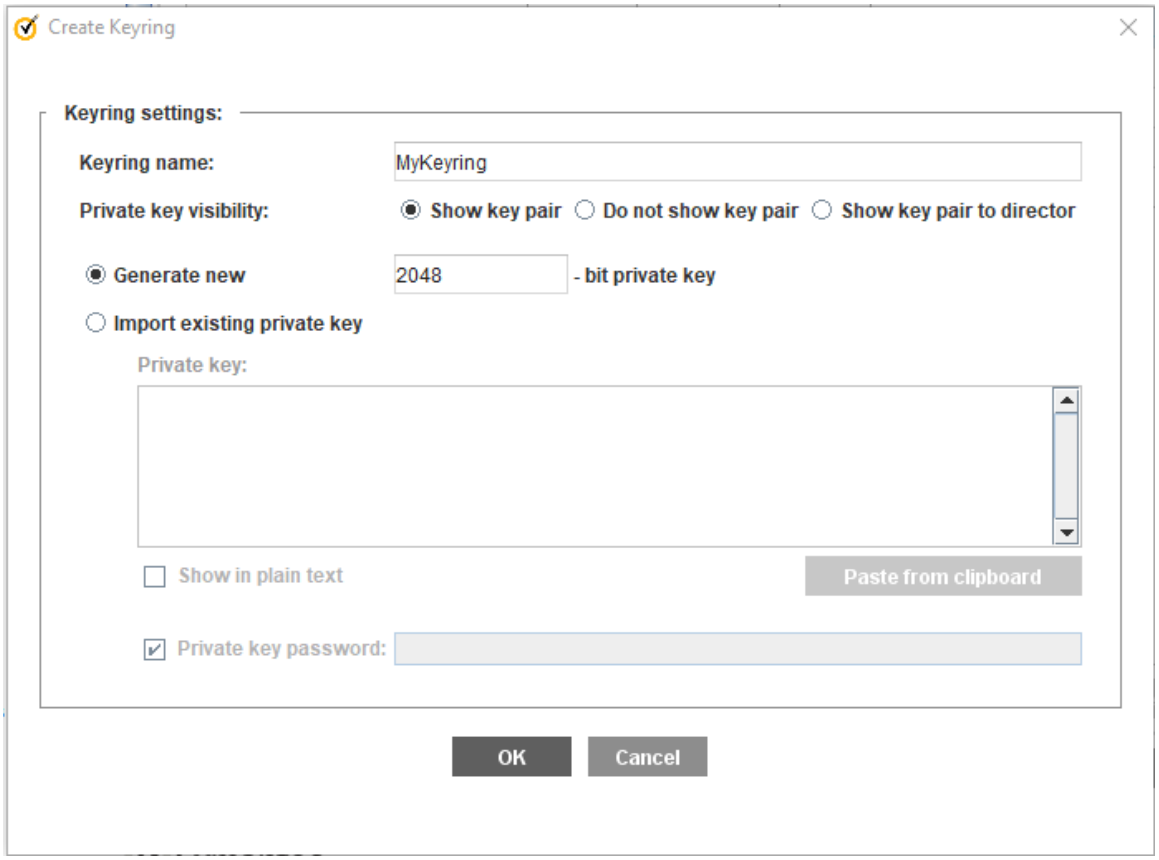
> **Tip:** If your network has servers or devices that require a direct connection to the Internet, use the **Static Bypass List** to define the IP addresses for those servers or clients to be exempted from proxy service interception.

Create an SSL Certificate Keyring

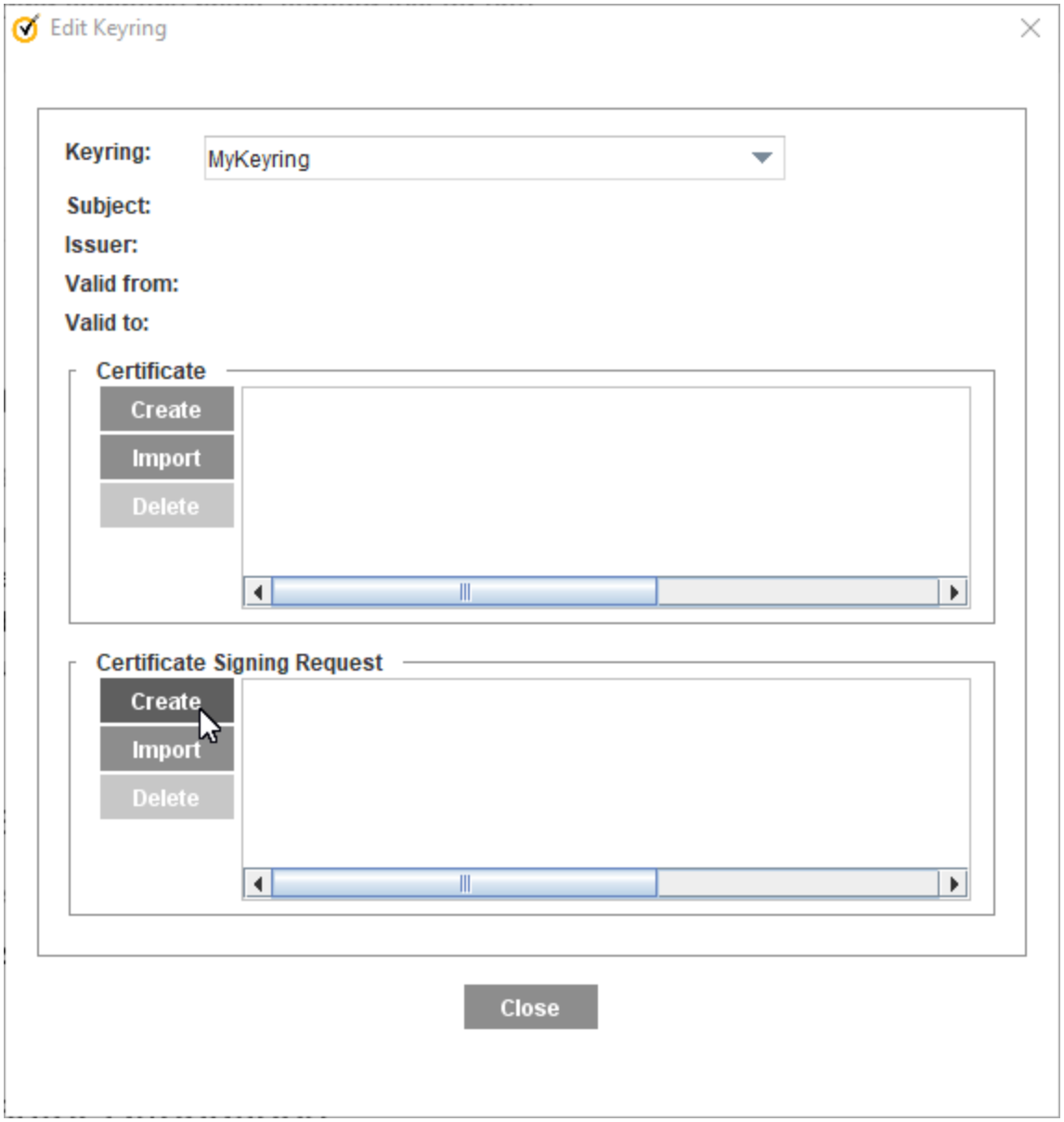
The ProxySG appliance uses a keyring to store certificates for HTTPS reverse proxy configurations. As users' HTTPS connections are terminated either before or on the appliance, you can choose whether traffic is sent using HTTP or HTTPS to your web servers.

To create an SSL certificate keyring:

1. Browse to the **Configuration > SSL > Keyrings** and click **Create**.

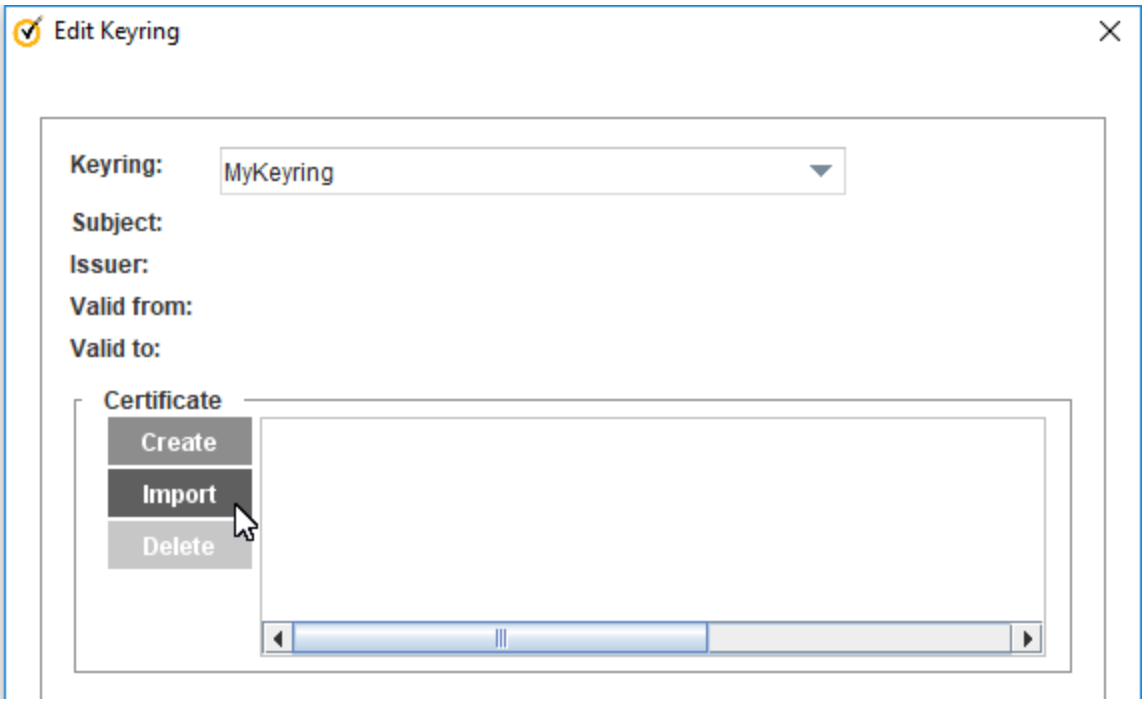


2. In the **Keyring name** field, type a name for the keyring.
3. Select **Show key pair** to permit backup and portability of the configuration.
4. In the **-bit private key** field, type the size for the key.
5. Click **OK** to create the keyring and commit the configuration to your appliance.
6. Select the keyring you created from the **Keyrings** list and click the **Edit** button.



7. In the **Certificate Signing Request** section, click **Create**. The Create Certificate Signing Request dialog displays.
8. Complete the form, paying close attention to the **Common Name** field. This should be a hostname or FQDN that resolves to the ProxySG appliance from outside of your protected network. This is the first step in ensuring that Internet-based browsers can trust the certificate the appliance presents. When you've completed the form, click **OK**, **Close**, and **Apply**.
9. Select the keyring and click **Edit** again. The Certificate Signing Request field contains a CSR in PKCS#10 format. Highlight the text from **-----BEGIN CERTIFICATE REQUEST-----** to **-----END CERTIFICATE REQUEST-----** and copy using **CTRL+C** (or on Apple systems, **the Apple key +C**) to copy the CSR to your system's clipboard.
10. Paste the CSR into a new text file on your local workstation and save the file with a .csr extension.

11. Send the CSR to be signed by a Certificate Authority (CA). The CA should provide you with a Root CA certificate as well as a server certificate. In some cases, an intermediate CA certificate is also provided.
12. Select the keyring and click **Edit** again.
13. In the **Certificate** section, click **Import**. The Import Certificate dialog opens. **Show screen.**

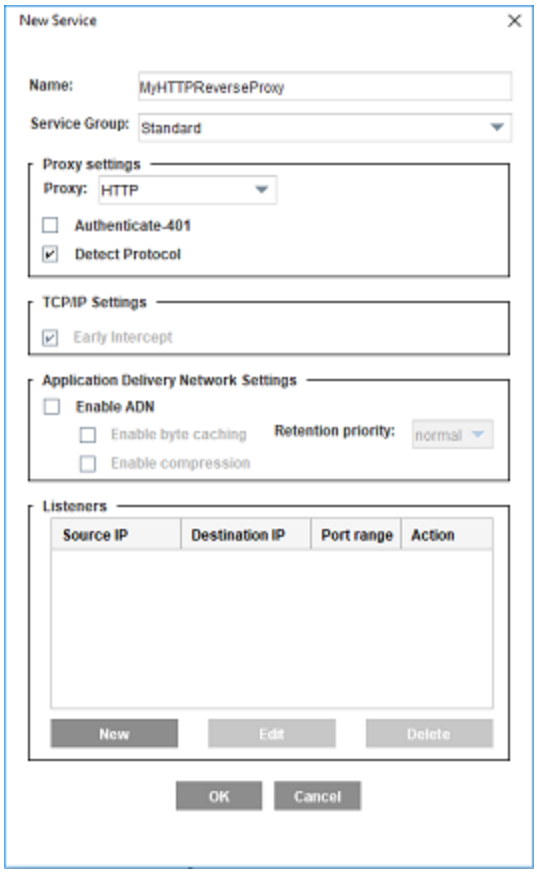


14. In the **Import Certificate** text box, paste the certificates in the order of first the server, then the intermediate, and then the CA certificate.
15. When all certificates have been entered into the text box, click **OK**, **Close**, and **Apply**.

Create an HTTP Service for Your Reverse Proxy

Configure an HTTP listener for your reverse proxy. This listener contains the IP address and TCP port that the ProxySG appliance uses to intercept traffic from the Internet or your edge firewall.

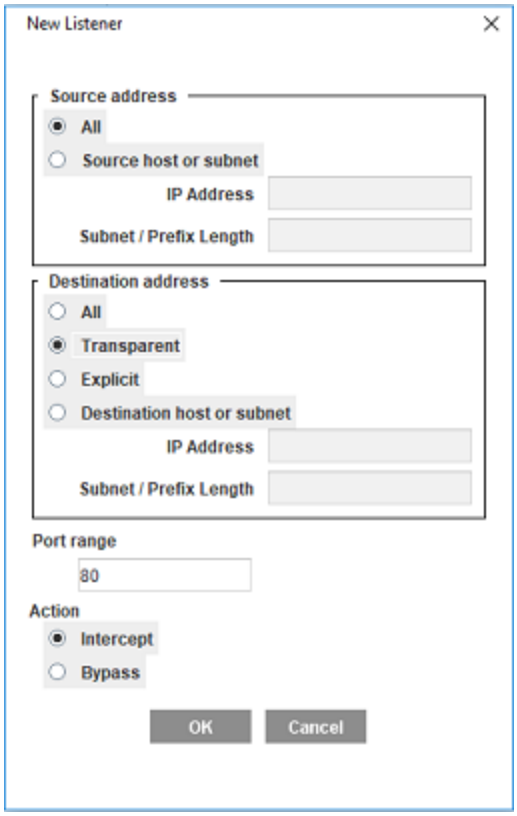
1. Log in to the Management Console.
2. Browse to **Configuration > Services > Proxy Services**.
3. Click the **New Service** button at the bottom of the page.



4. Type a name for the new service.
5. In the **Proxy** dropdown, select **HTTP** to handle simple HTTP-based websites. This proxy service type determines how the ProxySG appliance interprets and manages the traffic being passed through the service.
6. Enable **Detect Protocol**.
7. Ensure the **TCP/IP** parameter is set to **Early Intercept**. With early intercept, the ProxySG appliance returns a server acknowledgment back to the client and waits for the client acknowledgment, which completes the TCP 3-way

handshake before the appliance connects upstream to the server. For proxies that support object caching, the ProxySG appliance serves from the cache–a server connection is not necessary.

8. In the **Listeners** section, click **New**.

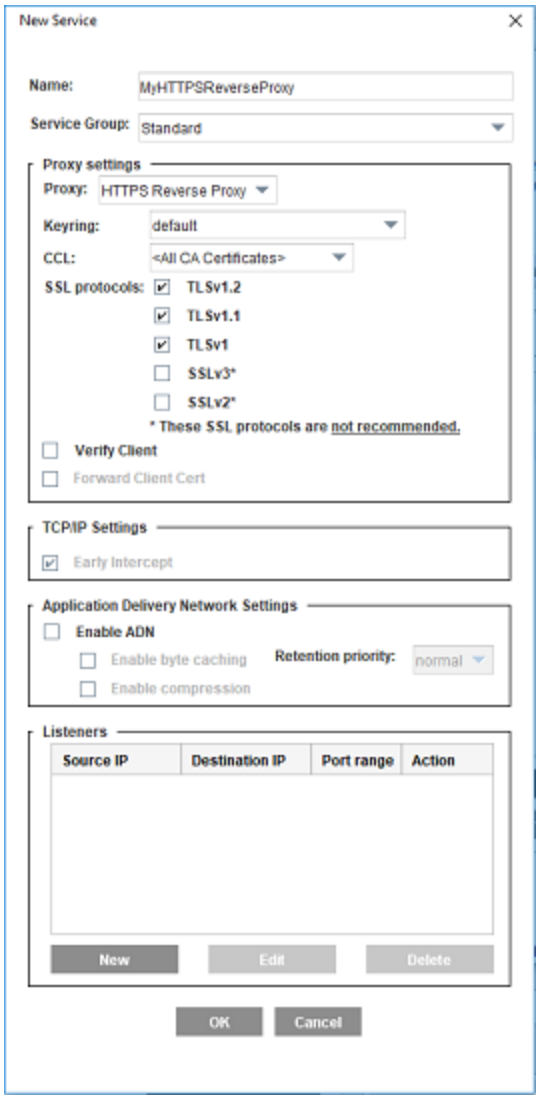


9. Unless your reverse proxy is deployed in a completely closed environment, Symantec recommends to leave the **Source Address** configuration at **All**. The **Source address** configuration is used to restrict the source of clients connecting through this service.
10. In the **Destination Address**, select **Transparent**.
11. In **Port range**, define a port or a range or ports that the appliance will monitor for connections. If you plan to add multiple ports to your configuration, define only one port number per service object and repeat for as many ports as necessary.
12. Set the **Action** to **Intercept**.
13. Click **OK**.
14. Click **OK**.
15. Click **Apply** to save the configuration.

Create an HTTPS Service for Your Reverse Proxy

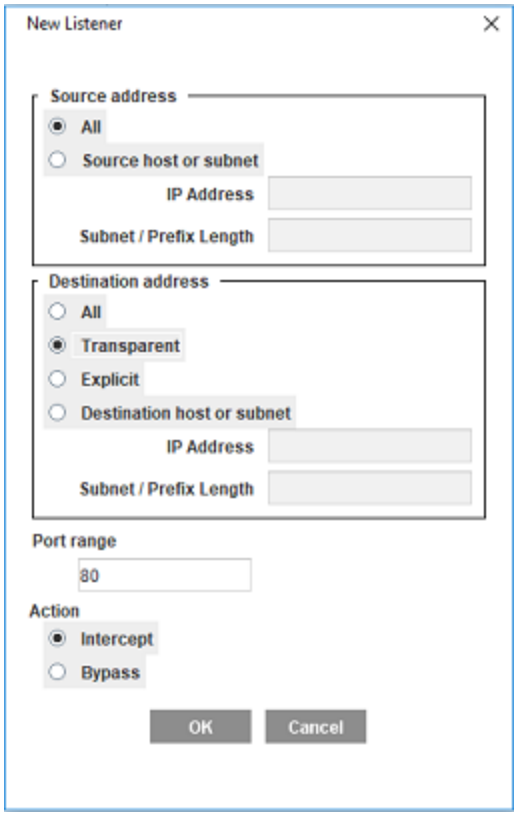
Configure a listener for your secure reverse proxy. This listener contains the IP address and TCP port that the ProxySG appliance uses to intercept traffic from the Internet or your edge firewall.

1. Log in to the Management Console.
2. Browse to the **Configuration > Services > Proxy Services**.
3. Click the **New Service** button at the bottom of the page.



4. Type a name for the new service.

5. In the **Proxy** drowdown, select **HTTPS Reverse Proxy** to handle secure HTTPS-based websites. This proxy service type determines how the ProxySG appliance interprets and manages the traffic being passed through the service.
6. Select the keyring you created for this configuration. If you have not created a keyring, "Create an SSL Certificate Keyring" on page 15.
7. In the **CCL** dropdown, select the CA Certificate List to be used to validate the certificate being presented to users. `<All CA Certificates>` is the default and suffices for most configurations.
8. Enable support for SSL protocols. SSLv3 and SSLv2 are not enabled by default as they are not recommended due to their insecure nature.
9. Disable ADN by deselecting the **Enable ADN** checkbox.
10. In the **Listeners** section, click **New**.



11. Unless your reverse proxy is deployed in a completely closed environment, Symantec recommends that you leave the **Source Address** configuration at **All**. The **Source Address** configuration is used to restrict the source of clients connecting through this service.
12. In the **Destination Address**, select **Transparent**.

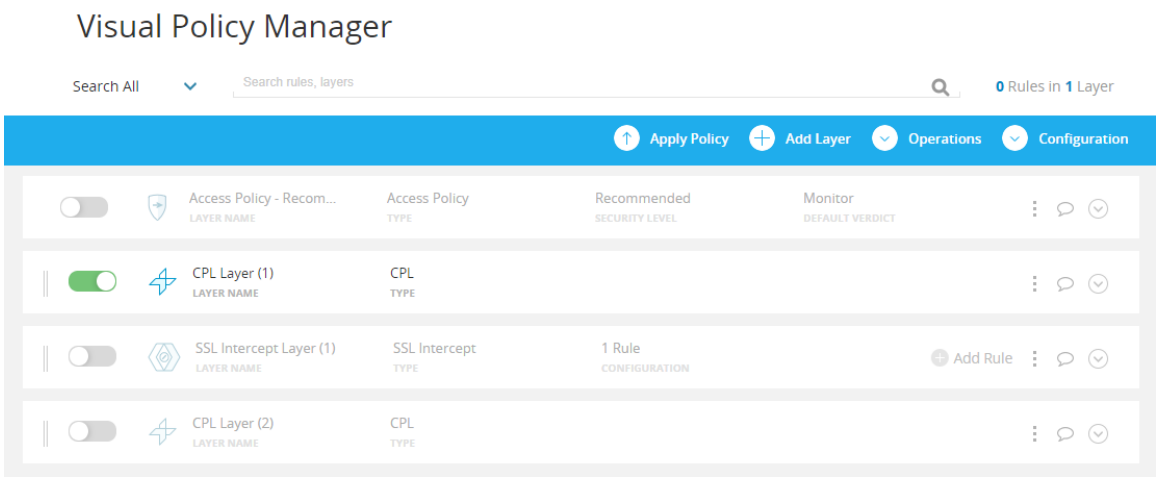
13. In **Port range**, define a port or a range or ports that the appliance will monitor for connections. For a standard HTTPS web server, type **443** as the port number. If you plan to add multiple ports to your configuration, define only one port number per service object and repeat for as many ports as necessary.
14. Set the **Action** to **Intercept**.
15. Click **OK**.
16. Click **OK**.
17. Click **Apply** to save the configuration.

Set Up an Allow Policy

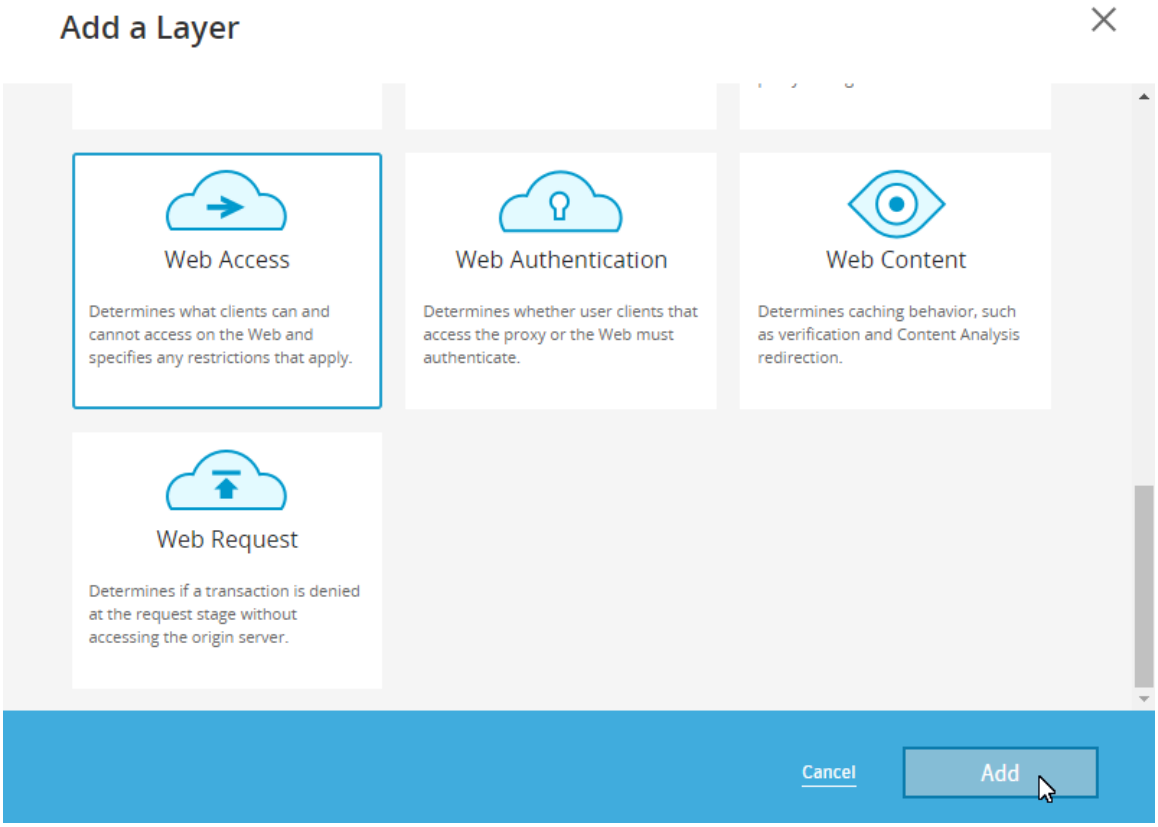
The ProxySG appliance uses policy to control how users on the Internet to access your content servers. Create policy to permit user access to your back-end content servers.

> **Note:** Before you begin, select the portal profile. If you have not enabled the portal profile, see "Enable the Portal Profile" on page 29.

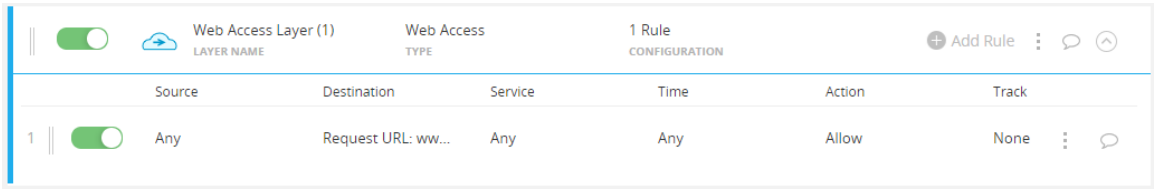
1. Log in to the Management Console.
2. Browse to **Configuration > Policy > Visual Policy Manager**.
3. Click **Launch VPM**.



4. Click **Add a Layer**.
5. Select **Web Access** and click **Add**. **Show screen.**



6. Type a name for the layer and click **OK**. The new layer appears at the bottom of the list of layers.
7. Under **Destination**, click the cell and click **Set**.
8. Click **Add new object** and select **Request URL**.
9. Select **Simple Match**.
10. In the **URL** field, type the domain name users use to access the website the reverse proxy will be servicing.
11. Click **Apply**.
12. Click **Set**.
13. For your new Web Access Layer, under **Action**, click the cell and click **Allow**.



14. Click **Apply policy** and click **OK**.

Next Step: You have completed the basic steps for deploying your reverse proxy. To further improve the effectiveness of your reverse proxy, you can "Enable the Portal Profile" on page 42, "Redirect Traffic Destined for the OCS" on page 61, "Configure the Reverse Proxy" on page 66, or "Maintain the Reverse Proxy by Analyzing Log Data" on page 81.

Enable Portal Profile

The HTTP Proxy portal profile acts as a server accelerator for the reverse proxy, and is used for web hosting. A server accelerator services requests meant for an OCS, as if it is the OCS itself.

To select the Portal Profile, go to **Management Console > Configuration > Proxy Settings > HTTP Proxy > Acceleration Profile**, and click **Use Portal Profile**.

Redirect Traffic Destined for the OCS

Ensure that traffic is being redirected to and from the ProxySG appliance properly by doing the following:

- Use Effective IP to Determine the Origin IP via the CLI or VPM

  If you rely on a deployment model where the client's real IP address is obscured by a load balancer or HTTP proxy (such as a reverse proxy indirect or forward proxy indirect deployment) and you want to extract the effective IP address, configure the appliance to use the value contained in the `X-Forwarded-For` header field or another custom header to identify the originating IP address.

- "Use Two-Way URL Rewrite to Redirect Traffic" on page 64

  If your configuration requires users on the Internet to input one URL and your internal web server accepts a different URL, you must configure the ProxySG appliance to use two-way URL rewrite policy to ensure proper traffic redirection.

- "Configure Load Balancing on the ProxySG Appliance" on page 65

  If your web server infrastructure uses multiple redundant servers to ensure uptime and reliability, configure the ProxySG appliance to distribute load between each server and tolerate failures by removing those servers that fail health checks.

Use Effective IP to Determine the Origin IP (CPL)

If you rely on a deployment model where the client's real IP address is obscured by a load balancer or HTTP proxy (such as a reverse proxy indirect or forward proxy indirect deployment) and you want to extract the effective IP address, configure the appliance to use the value contained in the `X-Forwarded-For` header field or another custom header to identify the originating IP address. To use the value defined in the header, you will need to specify the request header variable within policy.

> **Note:** The ProxySG appliance can only extract the effective IP address that is defined in the request header. If the request header is not present or contains an invalid address, the request uses the client IP address instead.

To configure the ProxySG appliance to extract the first IP address presented in the `X-Forwarded-For` header variable as the effective IP address, add the following policy:

```
<Proxy>
client.address=<ip_address> client.effective_address("$(request.header.X-Forwarded-For)")
```

where:

- *ip_address* specifies the HTTP proxy or load balancer IP address.
- `("$(request.header.X-Forwarded-For)")` is the effective IP address.

Alternatively, you can also use the VPM (Visual Policy Manager) to configure the ProxySG appliance to use the effective IP address of a client. See "Configure Effective IP Using the VPM" on the facing page

Configure Effective IP Using the VPM

You can also use the VPM to specify one or more request header substitutions to use to look up the effective client IP address, instead of using the CPL.

> **Note:** If you select or enter multiple substitutions, policy evaluates them in order of preference and uses the first substitution that evaluates to a valid IP address.

To specify one or more substitutions:

1. In the Management Console, browse to **Configuration > Policy > Visual Policy Manager**.
2. Click **Launch VPM**.
3. Click **Add Layer**.
4. Select **Web Access** and click **Add**.
5. Type a name for the layer and click **OK**.
6. For your new layer, in the **Action** column, click the cell and click **Set**.
7. Click **Add a new object**.
8. Click **Set Effective Client IP**.
9. Type a name for your object.
10. From the **Available** list, select one or more request header substitutions and move them to the **Selected - Order List**:
    - `$(request.header.X-Forwarded-For)` sets the address in the X-Forwarded-For header field as the client IP address.
    - `$(request.x_header.X-Client-IP)` sets the address in the X-Client-IP header field as the client IP address.
    - `$(request.header.Client-IP)` sets the address in the Client-IP header field as the client IP address.

    Alternatively, you can add a new substitution by clicking the add icon in the corner of the **Available** list.
11. Click **Apply**.
12. Click **Set**.
13. Click **OK**.

Use Two-Way URL Rewrite to Redirect Traffic

If your configuration requires users on the Internet to input one URL and your internal web server accepts a different URL, you must configure the ProxySG appliance to use two-way URL rewrite policy to ensure proper traffic redirection.

Two-way URL rewrite policy alters URLs from what the user on the internet inputs to what your internal servers accept. For more information, see the "define_url" definition reference in the *Content Policy Language Reference*.

Policy Example: Two-Way URL Rewrite Policy

In this example, users on the Internet access the page via https://portal.example.com/ while the web server URLs are defined as absolute links to http://internal.example.com/. For your scenario, simply replace the URLs with your own.

> **Note:** The publicly accessible URL that will direct users to the ProxySG appliance is first, while the second URL in the rewrite represents the URL the proxy will use to communicate with the web server.

```
define url_rewrite P
rewrite_url_prefix "https://portal.example.com/" "http://internal.example.com/"
end

define action portal
rewrite(url,"https://portal.example.com/(.*)","http://internal.example.com/$(1)")
transform P
end

define action force_uncompressed
delete (request.header.Accept-Encoding)
end

<Proxy>
url=https://portal.example.com/ action.portal(yes)

<Cache>
action.force_uncompressed(yes)
```

Configure Load Balancing on the ProxySG Appliance

If your web server infrastructure uses multiple redundant servers to ensure uptime and reliability, configure the ProxySG appliance to distribute load between each server and tolerate failures by removing those servers that fail health checks.

1. Configure each web server as a forwarding host. See "Create a Forwarding Host" on page 24.
2. Browse to **Configuration > Forwarding > Forwarding Hosts**.
3. Click the **Forwarding Groups** tab.
4. To create a new forwarding group, click **New**.
5. In the Members section, from the **Available Aliases** list, select each forward host and click **Add** to populate the Selected Aliases list.
6. Under **Load Balancing and Host Affinity**, define the load balance preferences:
    a. From the **Load balancing method** dropdown, select one of the options.
    b. In the **Host affinity methods** section, select an option for each method.
7. Click **OK** and then **Apply** to create the forwarding group.

Configure the Reverse Proxy

Configure your ProxySG reverse proxy solution to function within your unique environment and protect it from security threats.

Configure User Access to Your Web Servers

Configure who has access to the content on your web servers by configuring the ProxySG reverse proxy solution to authenticate users who are requesting access to those servers. In a reverse proxy deployment, to authenticate users:

1. **Determine the type of authentication realm your environment requires.** Based on your existing security infrastructure, select an authentication server type from the following table and see the corresponding chapter in the *SGOS Administration Guide*. After setting up an authentication realm, configure "Authentication Policy" on page 70 for the realm.

Authentication Realm Type	Administration Guide Chapter Reference
Local	"Local Realm Authentication and Authorization"
IWA	"Integrating Authentication with Active Directory Using IWA"
LDAP	"LDAP Realm Authentication and Authorization"
RADIUS	"RADIUS Realm Authentication and Authorization"
SAML	"SAML Authentication"

2. **Determine the authentication mode your environment requires.** In reverse proxy deployments, the ProxySG appliance issues OCS challenges. To reduce the amount of challenges sent, select an authentication mode to use authentication surrogates to cache authenticated sessions. For more information, see "About Authentication Modes" in the *SGOS Administration Guide*.

3. **Consider whether your environment requires a Server Name Indication (SNI) to service SSL/TLS requests.** If your environment has multiple applications on a web server, then use SNI to eliminate the need to create a service with a keyring for each server. For more information, see "Configure a Reverse Proxy with SNI in the Management Console" on the facing page

Configure a Reverse Proxy with SNI in the Management Console

If your environment has multiple applications on a web server, then configure your reverse proxy to use Server Name Indication (SNI) to service SSL/TLS requests. Using SNI eliminates the need to create a service with a keyring for each server. Instead, the reverse proxy uses a keylist with the `$(ServerName)` extractor in the configured service.

The SNI configuration, including keylist selection, can also be configured through the Command Line Interface. See "Use CLI to Configure a Reverse Proxy with SNI" on the next page.

To configure a reverse proxy with SNI:

> **Note:** Existing reverse proxy services can be consolidated by creating keylists with the `$(ServerName)` extractor.

1. Create keyrings for the web applications. See the "Creating a Keyring" section in the *SGOS Administration Guide*.

   > **Note:** HSM keyrings and keygroups are not supported.

2. Create a keylist with the `$(ServerName)` extractor. See the "Group Related Client Keyrings into a Keylist" section in the *SGOS Administration Guide*.
3. Create an HTTPS service that specifies the keylist for the reverse proxy service. See "Create an HTTPS Service for Your Reverse Proxy" on page 54.
4. Write forwarding rules for the web application. See "Set Up an Allow Policy" on page 57.

Use CLI to Configure a Reverse Proxy with SNI

The SNI configuration is available through the Management Console as well as with the Command Line Interface (CLI). See the *Command Line Interface Reference* for information on using the CLI.

To configure a reverse proxy with SNI using the CLI:

> **Note:** Existing reverse proxy services can be consolidated by creating keylists with the $(ServerName) extractor.

1. Create a keylist with the `$(ServerName)` extractor.
   Example:
   ```
   #(config ssl) create keylist <my_keylist>
   #(config ssl) edit keylist <my_keylist>
   #(config ssl keylist my_keylist) extractor $(ServerName)
   ```
   For more information, see the "#(config) ssl" reference in the *Command Line Reference*.
2. Specify the keylist for the reverse proxy service.
   - If you are creating a new service, use:
     `#(conf proxy-services) create https-reverse-proxy <service-name> <service-group> [<keyring>|<keylist>]`
   - If you are modifying an existing https-reverse-proxy to use a keylist, use:
     `#(conf rps1) attribute keyring <keyring-id>|<keylist>`, where "rps1" is the name of the service.

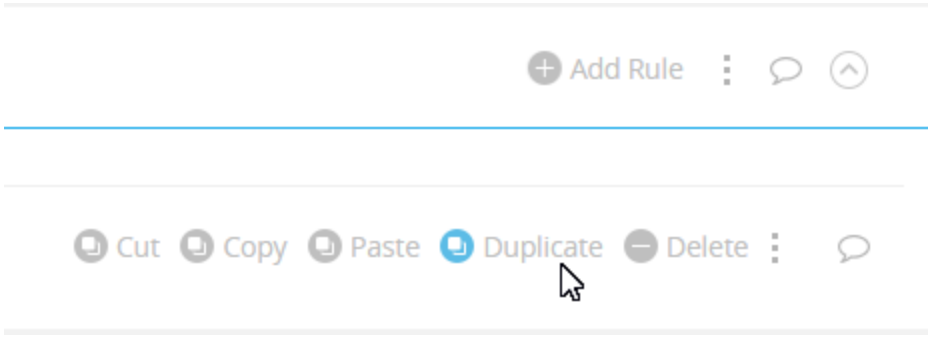
     For more information, see the "#(config) proxy-services" reference in the *Command Line Reference*.
3. Write forwarding rules for the backend. See "Set Up an Allow Policy" on page 57.

Authentication Policy

With an authentication realm configured, you can configure policy on the ProxySG appliance to authenticate, log, and control user access to your web server.

Configure policy to:

- **Create a rule to authenticate users.** See the "Configuring Authentication-Based Access Privileges " section in the *SGOS Administration Guide*.
- **Secure your existing Web Access rules:**
  1. In the VPM (**Configuration > Policy > Visual Policy Manager** and **Launch VPM**), browse to your **Web Access Layer**.
  2. Identify the rule that permits users to access your web server.
  3. In the **Source** column, click the cell and click **Set**.
  4. Click **Add a new object** and select **Group**.
  5. Enter the group for the type of authentication realm you're using.
  6. Click **Apply**.
  7. Click **Set**.
  8. Click **Apply Policy**.
- **Prevent unauthorized access:**
  1. In the Web Access Layer, duplicate the existing rule.



  2. In the **Source** column, click the cell and click **Negate**.
  3. In the **Action** column, click the cell and click **Deny**.
  4. Click **Apply Policy** and click **OK**.

Optimize Reverse Proxy Performance

Configure a Portal Profile to enable your reverse proxy to act as a server accelerator. See the "About the Portal Profile" and "Configuring the HTTP Proxy Profile" sections in the *SGOS Administration Guide*.

Configure Web Application Firewall

If you have a Web Application Firewall subscription for your ProxySG appliance, configure Web Application Firewall policy to detect and prevent attacks on your web-based application. For more information about Web Application Firewall policy and steps on configuring it, see the *SGOS Web Application Firewall Solutions Guide*. If you also have Management Center, see *Management Center Web Application Firewall Policy Guide*.

Modify the Parameters for SSL Connections

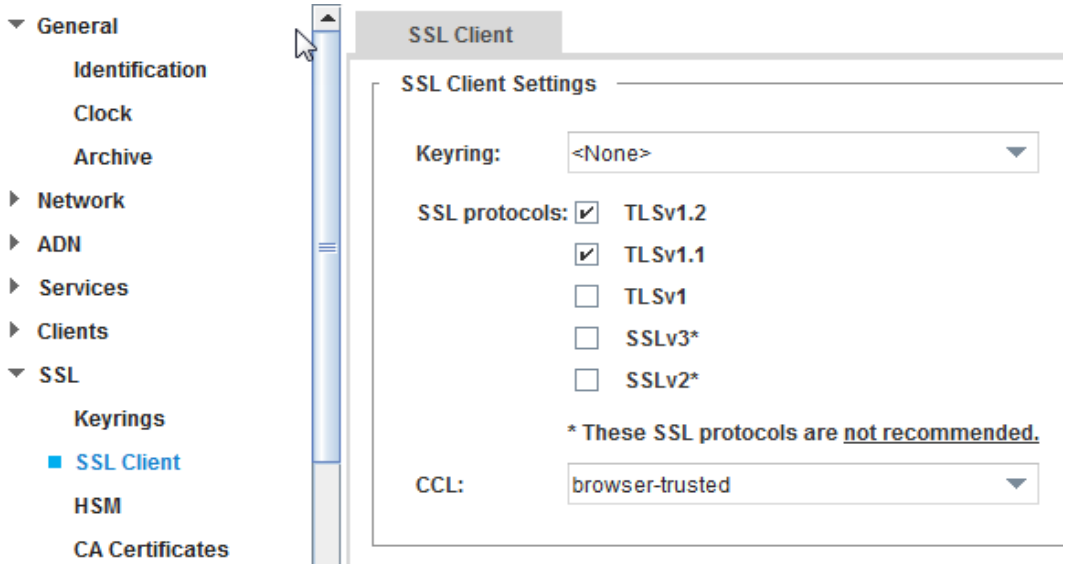
To modify parameters for SSL connections in a reverse proxy scenario, modify the SSL client profile. The reverse proxy uses the SSL client profile when using HTTPS to connect to the upstream OCS.

The SSL client settings are global, affecting all services that use it. Unless required by your environment, you do not need to change any settings. The default settings for the SSL client profile are:

- **Keyring:** None
- **SSL Versions:** TLSv1.1, TLSv1.2
- **CCL:** browser-trusted
- **Cipher suite:** A selection of ciphers Symantec considers sufficiently secure; see the next section.

To modify the SSL client profile:

1. Select **Configuration > SSL > SSL Client**.



2. For the SSL Client Settings, do the following:

   a. If the server in question requires a client certificate, from the **Keyring** dropdown, select the keyring used to negotiate with origin content servers through an encrypted connection. Only keyrings with certificates can be associated with the SSL client. By default, no keyring is selected.

   b. (Optional) For the **SSL Protocols** checkboxes, select the correct SSL versions for your environment. The defaults are **TLSv1.2** and **TLSv1.1**.

c. From the **CCL** dropdown, select the CCL that the appliance uses to determine which CA certificates are trusted during server certificate validation. The CCL can be any already created certificate list. By default, the browser-trusted CCL is used.

3. Click **Apply**

4. (Optional) Change the cipher suite. See "Change the SSL Client Cipher Suite" on the next page.

Change the SSL Client Cipher Suite

The cipher suite sets the encryption method for the ProxySG appliance. You can only change the cipher suite via the CLI. For more information, see *Command Line Reference*.

Change the Cipher Suite of the SSL Client

> **Note:** Some cipher suites that Symantec considers to be insufficiently secure are disabled by default for the SSL client. If you enable insecure cipher suites, you can use the `#(config ssl ssl-client default)restore-settings` command to restore the default settings, including the originally disabled ciphers. To identify disabled ciphers, look for "no" in the Use column in CLI output. You can enable these ciphers if desired.

1. Select the ciphers you want to use at the prompt.

```
#(config) ssl
#(config ssl) edit ssl-client ssl_client_name
#(config ssl ssl-client ssl_client_name) cipher-suite
Select cipher numbers to use, separated by commas: 1,3,4
ok
```

2. (Optional) View the results.

```
#(config ssl ssl-client ssl_client_name) view
SSL-Client: default
Keyring: <None>
CCL: browser-trusted
Protocol: tlsv1 tlsv1.1 tlsv1.2
Cipher suite: ecdhe-rsa-aes256-sha384 ecdhe-rsa-aes256-gcm-sha384 ecdhe-rsa-aes128-gcm-256
```

Non-Interactively Change the Cipher Suite of the SSL Client

Enter the following commands:

```
#(config) ssl
#(config ssl) edit ssl-client ssl_client_name
#(config ssl ssl-client ssl_client_name) cipher-suite cipher
```

where *cipher* is any of the of the available cipher suites.

Notes:

- If you do not specify any attributes, the cipher suite cannot be used.
- Multiple ciphers can be specified on the command line, separated by blank spaces.

Example

```
#(config ssl ssl-client default) cipher-suite rc4-sha
ok
#(config ssl ssl-client default) view
SSL-Client: default
Keyring: <None>
CCL: browser-trusted
Protocol: tlsv1 tlsv1.1 tlsv1.2
Cipher suite: rc4-sha
```

Configure Multi-Tenant Policy

If you want to enforce unique sets of policy on distinct groups of users, use multi-tenant policy. For information on how multi-tenant policy works, licensing, and policy examples, see the *Multi-Tenant Policy Deployment Guide*.

Reverse Proxy Logging: About the bcreporterwarp_v1 Access Log

As user traffic passes through your reverse proxy, their activities are logged to the bcreporterwarp_v1 access log. The ProxySG appliance sends user data at configured intervals to an upload client that you configure (such as Blue Coat Reporter or Splunk).

For more information on logging, see the *SGOS Administration Guide*.

For information on interpreting access logs, see the *SGOS Web Application Firewall Solutions Guide*.

Format of the bcreporterwarp_v1 Access Log

The bcreporterwarp_v1 format is a reserved format and cannot be edited. The format is the following access logging fields:

```
date time time-taken c-ip cs-username cs-auth-group x-bluecoat-transaction-uuid x-exception-id cs(Referer) sc-status s-action cs-method rs(Content-Type) cs-uri-scheme cs-host cs-uri-port cs-uri-path cs-uri-query cs-uri-extension cs(User-Agent) s-ip sc-bytes cs-bytes x-virus-id x-cs-client-ip-country x-user-x509-serial-number x-user-x509-subject rs-bytes x-cs-client-effective-ip x-cs-client-effective-ip-country cs(X-Forwarded-For) rs-service-latency r-ip x-bluecoat-application-name x-bluecoat-waf-attack-family x-risk-scorex bluecoat-waf-block-details x-bluecoat-waf-monitor-details x-bluecoat-request-details-header x-bluecoat-request-details-body x-bluecoat-waf-scan-info
```

CLI Commands

The following CLI commands are relevant to this access log:

```
access-log
edit log main
format-name bcreporterwarp_v1
```

For more information, see the *Command Line Reference*.

Access Log Field Details

The following table shows the name, description, and the software release the field was introduced in.

For information on access log properties, see the *Content Policy Language Reference*.

> **Tip:** Enabling full request logging (body, header) for all requests greatly increases the access log size. Symantec suggests sending the details to a second log stream. Use the transaction ID (`x-bluecoat-transaction-uuid`) to correlate log lines.

Name	Description	Introduced in log
date	GMT date in YYYY-MM-DD format.	6.5.5.7

Name	Description	Introduced in log
time	GMT time in HH:MM:SS format	6.5.5.7
time-taken	Time taken (in milliseconds) to process the request (from the first byte of client request data received by the proxy, to the last byte sent by the proxy to the client, including all of the delays by ICAP, and so on).	6.5.5.7
c-ip	Client IP address.	6.5.5.7
cs-username	Relative username of a client authenticated to the proxy (i.e. not fully distinguished).	6.5.5.7
cs-auth-group	One group that an authenticated user belongs to. If a user belongs to multiple groups, the group logged is determined by the Group Log Order configuration specified in VPM. If Group Log Order is not specified, an arbitrary group is logged. Only groups referenced by policy are considered.	6.5.5.7
x-bluecoat-transaction-id	Unique per-request transaction ID generated by the appliance.	6.6.2.1
x-bluecoat-transaction-uuid	Globally unique per-request transaction ID that can be identified across ProxySG appliances.	6.6.3.1
x-exception-id	Identifier of the exception resolved (empty if the transaction has not been terminated).	6.5.5.7
cs(Referer)	Request header: Referer.	6.5.5.7
sc-status	Protocol status code from appliance to client.	6.5.5.7
s-action	What type of action did the appliance take to process this request (including WAF cache hit/miss); possible values include ALLOWED, DENIED, FAILED, SERVER_ERROR.	6.5.5.7
cs-method	Request method used from client to appliance.	6.5.5.7
rs(Content-Type)	Response header: Content-Type.	6.5.5.7
cs-uri-scheme	Scheme from the 'log' URL.	6.5.5.7
cs-host	Hostname from the client's request URL. If URL rewrite policies are used, this field's value is derived from the 'log' URL.	6.5.5.7
cs-uri-port	Port from the 'log' URL.	6.5.5.7
cs-uri-path	Path from the 'log' URL. Does not include query.	6.5.5.7
cs-uri-query	Query from the 'log' URL.	6.5.5.7
cs-uri-extension	Document extension from the 'log' URL.	6.5.5.7
cs(User-Agent)	Request header: User-Agent.	6.5.5.7
s-ip	IP address of the appliance on which the client established its connection.	6.5.5.7

Name	Description	Introduced in log
sc-bytes	Number of bytes sent from appliance to client.	6.5.5.7
cs-bytes	Number of bytes sent from client to appliance.	6.5.5.7
x-virus-id	Identifier of a virus if one was detected.	6.5.5.7
x-cs-client-ip-country	Client country of origin.	6.5.5.7
x-user-x509-serial-number	X.509 certificate serial number.	6.5.5.7
x-user-x509-subject	X.509 certificate subject.	6.5.5.7
rs-bytes	Number of bytes sent from upstream host to appliance.	6.5.5.7
x-cs-client-effective-ip	In load balancing environments, reports actual client IP address	6.5.5.7
x-cs-client-effective-ip-country	In load balancing environments, reports actual client country of origin.	6.5.5.7
cs(X-Forwarded-For)	In multi-layer proxy deployments, reports the forwarding proxy.	6.5.5.7
rs-service-latency	OCS response time. The time from the start of the OCS connection to when the ProxySG appliance receives the first response byte.	6.6.2.1
r-ip	IP address from the outbound server URL.	6.5.5.7
x-bluecoat-application-name	Reports the application name.	6.6.2.1
x-bluecoat-waf-attack-family	Natural language description of the detected attack family.	6.6.2.1
x-risk-score	Risk score.	6.5.5.7
x-bluecoat-waf-block-details	Details about the blocked or monitored request. See "New and Updated CPL" on page 13 for information on the block and monitor actions.	6.6.2.1
x-bluecoat-waf-monitor-details		6.6.2.1
x-bluecoat-request-details-header*	All HTTP header content from user requests: method, URI, version, headers (including all header content up to the body of an HTTP request).	6.7.4.1
x-bluecoat-request-details-body*	HTTP body from user requests.	6.7.4.1
x-bluecoat-waf-scan-info	Indicates if WAF processing was applied to the request. WAF processing may not be applied if WAF is disabled, or if the response was served from the response cache and the WAF cache hit optimization is enabled.	6.7.4.1

* These two logs are suppressed by default. Create or enable policy to unsuppress.

Maintain the Reverse Proxy by Analyzing Log Data

The Blue Coat WAF App for Splunk® Enterprise 6 provides several dashboards to visualize data from ProxySG Web Application Firewall (WAF) logs. You can use this data to see which policies and configurations are effective, and areas that could be refined. Use the app to aggregate log data passed into the database and specify how the log data is sorted. You can also search log files based on various criteria using a built-in pivot search against Blue Coat Security Analytics.

Refer to the *Blue Coat ProxySG Web Application Firewall (WAF) App for Splunk Enterprise Product Installation Guide* for details.

Supporting Documentation

The following supporting documentation for SGOS is available.

Title	Overview
SGOS Administration Guide	Provides reference information and procedures for administrators to configure the ProxySG appliance.
Authentication WebGuide	How to integrate ProxySG authentication with AD using IWA, AD using Windows SSO, AD using LDAP, and SAML.
Command Line Reference	Commands available in the ProxySG appliance CLI and how to use them to perform configuration and management tasks.
Content Policy Language Reference	CPL gestures available for writing the policy by which the ProxySG appliance evaluates web requests.
Knowledge Base	Contains articles and documentation to help you troubleshoot your ProxySG appliance.
Multi-Tenant Policy Deployment Guide	Working with Multi-Tenant Policy configurations to segregate policy for distinct groups of users.
ProxySG First Steps WebGuide	How to deploy a ProxySG appliance.
ProxySG Security Best Practices Guide	Provides best practices to consider when constructing ProxySG appliance/SGOS policy.
SGOS Release Notes	Changes, issues, fixes, and limitations pertaining to SGOS releases. Also includes any related security advisory (SA) fixes.
Required ports, protocols, and services for ProxySGappliance	View lists of ports and services used by each Symantec Network Protection Product.
SSL Proxy Deployment Guide	Best practices for deploying the SSL proxy. The SSL proxy improves visibility into SSL traffic, allowing security policies and logging to be applied to encrypted requests and responses, and can enhance performance by caching encrypted data.
SGOS Upgrade/Downgrade Guide	Steps for upgrading or downgrading SGOS. Also covers behavior changes and policy deprecations.
Web Visual Policy Manager Reference	How to create and implement policy in the ProxySG appliance's Web Visual Policy Manager, including layer interactions, object descriptions, and advanced tasks.
Legacy Visual Policy Manager Reference	Describes how to create and implement policy in the ProxySG appliance's legacy Visual Policy Manager, including layer interactions, object descriptions, and advanced tasks.

SGOS Web Application Firewall Solutions Guide	How to configure Symantec's WAF solution to protect your web servers, accelerate web content, and simplify operation.
Management Center Web Application Firewall Policy Guide	How to configure Symantec's WAF solution to protect your web servers, accelerate web content, and simplify operation.