Securing Outlook Web Access

Introduction

Outlook Web Access (OWA) offers simple and convenient access to corporate email accounts by using a Web browser on any system from any Internet-connected location. Web access from any location, however, introduces security issues such as maintaining information confidentiality, avoiding improper logoffs, removing content left in memory, and providing secure authentication. OWA also places a burden on the server side by using approximately 4MB of memory per user to serve up Web-based email, not to mention the overhead generated by encrypted traffic.

The Blue Coat ProxySG serves as the basis for a robust and flexible solution to front-end Microsoft’s OWA product and provides the necessary security needed by today’s enterprises. In addition to Web policy management, content filtering, virus-scanning and network protection, companies can implement a scalable and secured Outlook Web Access service using the ProxySG. The ProxySG solution offers encryption of data along with an automatic inactivity timeout enabling administrators to more fully secure access from public networks. This Technical Brief describes how to implement a secure solution for Outlook Web Access using the ProxySG to intercept OWA traffic before it reaches the mail server.

Implementing Secured Outlook Web Access

There are two parts to securing Outlook Web Access using the ProxySG:

1. Provide HTTPS termination on the ProxySG
2. Implement an inactivity timer

The following diagram represents the solution for securing Outlook Web Access using the Blue Coat ProxySG.

![Diagram of secured Outlook Web Access](image)

The following sections describe how to create a Secured OWA service on the ProxySG.

NOTE: In the following examples, the URL “webmail.example.com” is used as the OWA Internet URL, and 1.2.3.4 is used as the OWA server’s IP address. As you do the procedures, use your own OWA Internet URL and OWA server’s IP address. This procedure assumes a DNS-based reverse proxy setup, where the hostname, “webmail.example.com” in the procedures, resolves to an externally reachable IP address on the reverse proxy.

Part 1 – Implementing HTTPS termination

Four tasks must be completed to implement HTTPS termination on the ProxySG:

1. Configuring the SSL Keyring and Certificate
2. Configuring Advanced Forwarding Hosts
3. Adding the HTTP Header (front-end HTTPS)
4. Configuring Advanced Forwarding Rules
Part 1, Task 1 – Configuring the SSL Keyring and Certificate

1. Open the Blue Coat management console on the ProxySG and go to SSL > Keyrings as shown above.

2. Click Create; the Create Keyring dialog displays. In this example the keyring is named “sslserver”. Click OK to create the keyring and dismiss the dialog. Click Apply in the management console. Click OK to dismiss the confirmation dialog.

   NOTE: If you are going to import a certificate in the next step, then import the keyring for the certificate in this step.
Next, create or import a certificate for the new keyring. To do this, select the new keyring and click **Edit/View**.

**NOTE:** A self-signed certificate can be used (which may cause warnings in the browser) or a request can be made with the **Certificate Signing Request** option to a valid CA authority that will then return a signed certificate understood by most browsers. This example creates a self-signed certificate.

Click **Create** in the **Certificate** area and fill in the form. Alternatively, if you want to use a CA certificate and have a signed certificate that you can import into the ProxySG, click **Create** in the **Certificate Signing Request area** instead.

Note: The **Common Name** option is the URL of the OWA that users enter. This example uses **webmail.example.com**.

Click **OK** to finish. The dialog goes away and your data is displayed; if satisfied, click **Close**. Click **Apply** in the management console. Click **OK** to dismiss the confirmation dialog.
To view the encrypted key, click **Edit/View**, the encrypted certificate displays; example above. Click **Close** to dismiss the window.

![SSL Certificates window](image)

Next, the keyring must be assigned to an HTTPS Reverse Proxy service on the ProxySG: From the Blue Coat management console go to **Services > Proxy Services** as shown above.
Select the HTTPS service and click Edit. Select HTTPS Reverse Proxy from the Proxy dropdown menu to display additional options. Select the previously defined certificate for the Keyring option (sslserver in the example).

Ensure that the Listener Destination address is set to Explicit and the action is set to Intercept. Click New to create a new listener if needed, or click Edit to modify an existing one. Click OK to dismiss the Listener dialog. Click OK to dismiss the Edit Service dialog; click Apply in the Management Console. Click OK to dismiss the confirmation dialog.
Part 1, Task 2 – Configuring Advanced Forwarding Hosts
The second task in this process is to define the location of the back-end server[s] to obtain the email content.

From the management console, go to **Forwarding > Forwarding Hosts** as shown above.

Give the forwarding host an **Alias**, this example uses **mywebserver1**, and enter the IP address of your OWA server as the **Host**.
Part 1, Task 3 – Adding the HTTP header (front-end-https)

Launch the Visual Policy Manager (VPM) to add the HTTP header [front-end-https] to the packet when sending requests to the Outlook Web Access server, and to allow HTTPS traffic. This is achieved by creating a Web Access Layer in the VPM as shown in the following steps.

NOTE: The URL “webmail.example.com” used in this procedure should be replaced with the URL of your OWA.

1. Click **Apply** to finish.

2. Begin by right-clicking **Policy** and selecting **Add Web Access Layer** from the drop-down list. Name the layer, if you wish and click **OK**. This example uses the default name.
1. Right-click the **Destination** setting and select **Set**. The Set Destination dialog displays.

2. Click **New** and select **Request URL**. The Add Request URL Object dialog displays. Click **Advanced Match** and select **Any** for **Scheme**. Enter the host name of your OWA server for the **Host**. Name the object if you wish, this example names it **RequestURL_HttpsOWA**. Click **Add** to add the object (wait until the dialog clears); click **Close** to dismiss the dialog. The Set Destination Object dialog re-displays with the new object.
Click OK to set the object and dismiss the dialog. The VPM re-displays with the new **Destination** setting.

Next, right-click the **Action** setting and select **Set**. The Set Action Dialog displays.

Click **New** and select **Combined Action Object**. The Add Combined Action Object dialog displays.
Click **New** and select **Control Request Header**. The Add Control Request Header Object dialog displays.

For the **Header Name** option, select **Front-End-HTTPS** from the dropdown menu. Select **Set value** and enter **ON** as the value. Name the object if you wish; this example names the object **FrontEndHttps**.

Click **OK** to dismiss the dialog. The Add Combined Action Object dialog re-displays.

Select the Control Request Header object that you just created and the **Allow** object (at the top of the list), one at a time, and move them to the **Selected Action Objects** box by clicking **Add>>**, as shown above. Name the object if you wish; this example names it **FrontEndHttpsAllow**.
Click **OK** to add the combined action object and dismiss the dialog. The Set Action Object dialog re-displays.

Click **OK** to set the combined action object. The VPM displays the configured Web Access layer as shown above. Click **Install Policy** to install the Web Access Layer to the policy. Click **OK** to dismiss the confirmation dialog.

Keep the VPM open for the next procedure.
Part 1, Task 4 – Configuring Advanced Forwarding Rules

Next, add the forwarding rules to send requests to the OWA server.

1. Begin by right-clicking **Policy** and selecting **Add Forwarding Layer** from the dropdown menu; this example names the layer **Forwarding**. Click **OK** to add the new layer.

2. Right-click the **Destination** setting and select **Set**. The Set Destination Object dialog displays.

3. Click **New** and select **Server URL**. The Add Server URL Object dialog displays.
Click **Advanced Match**, select **https** as the **Scheme**, and enter the URL of your OWA as the **Host**. Name the object if you wish; this example uses the same name as the OWA URL. Click **Add** to add the Server URL object (wait until the dialog clears). Click **Close** to dismiss the dialog. The Set Destination Object dialog re-displays.

Click **OK** to set the object and dismiss the dialog. The new destination object displays in the forwarding layer.

Next, define forwarding of Web requests to your OWA server to the appropriate mail server: Right-click the **Action** setting and select **Set**. The Set Action Object dialog displays.
Click **New** and select **Select Forwarding**. The Add Select Forwarding Object dialog displays.

Select your previously-defined forwarding host (mywebserver1, in the example) and click **Add** to move it from the left-hand box to the right-hand box. Name the forwarding object if you wish; this example names the object “mywebserver1.” Click **OK** to add the object and dismiss the dialog. The Set Action Object dialog re-displays.
Click OK to set the object and dismiss the dialog. The VPM displays the configured forwarding layer as shown below.

Click Install Policy to install the forwarding policy. Click OK to dismiss the confirmation dialog. Close the VPM window.

Part 2 – Implement an Inactivity Timer

An inactivity timer causes the session from a browser to the ProxySG to shut down after a set period of time. This feature adds greater security in environments where users are accessing their Outlook email from a public network. There are three tasks to implementing an inactivity timeout:

1. Download and Modify the Exceptions and Policy Zip File
2. Install Custom Exceptions
3. Install the Modified Policy

IMPORTANT! You will use a Blue Coat-provided zip file that contains two files: one for the exceptions and one for the policy. You will need to download, unzip, and modify each file before installing.

Part 2, Task 1 - Download and Modify the Exceptions and Policy Zip File

Download the following pre-defined Blue Coat zip file to your local PC by going to the following link:

http://www.bluecoat.com/doc/direct/7979

Unzip the file after downloading. There will be two files: securing_owa_cpl_exceptions.txt and securing_owa_cpl_policy.txt. Save them to your PC for installation.

Open each file and modify as instructed at the top of each. You need to use the URL of your OWA server and, optionally, change the timeout value from 2 minutes to what you want.

Save each file for installation in the following procedures.
Part 2, Task 2 – Install Custom Exceptions
The following exceptions need to be installed on the ProxySG, instructions follow:

- **OWA Login Exception**: Displays a splash page telling users they are logging in to OWA.
- **OWA Logoff Exception**: Causes OWA to display a “session has timed out” warning to users.

1. Go to **General > Archive** in the Management Console as shown above.
2. In the Install Configuration area, leave **Local File** selected and click **Install**. A file Open dialog displays.
3. Select the securing_owa_cpl_exceptions.txt file that you saved to your PC and modified, and click **Open**.
4. Click **OK** to dismiss the confirmation dialog.
Part 2, Task 3 – Install the Modified Policy

1. To install the policy to your ProxySG, open the Management Console. Go to Configuration > Policy > Policy Files.

2. In the Install Policy area, Install Local File from option, select Local File and click Install. An Open dialog displays.

3. Select the securing_owa_cpl_policy.txt file that you saved to your PC and modified, and click Open.

4. Click OK to dismiss the confirmation dialog.
Testing the Secured Outlook Web Access

Open a Web browser to the OWA server in the policy. The client connects to the Secured OWA server.

The client can view OWA email using any Web browser through the ProxySG.
When the session has timed out due to inactivity the following message appears:

Adding a Re-direct

To add a re-direct for "webmail.example.com" or "http://webmail.example.com," to "https://webmail.example.com," follow these steps.

1. In the Visual Policy Manager, select the Web Access Layer that you defined and click Add Rule.
Click **Move Rule** to place the new rule above the existing one.

Right-click the **Destination** setting and select **Set**. The Set Destination Object dialog displays.

Select the previously defined destination object and click **OK**. The VPM re-displays.
Next, right-click the Service setting and select Set. The Set Service Object dialog displays.

Click New and select Client Protocol. The Add Client Protocol object dialog displays.

In the top drop-down list, select HTTP. Click OK to add the object and dismiss the dialog.

The Set Service Object dialog re-displays.
9. Click **OK** to set the object and dismiss the dialog. The VPM re-displays.

10. Now, right-click the **Action** setting and select **Set**. The Set Action Object dialog displays.

11. Click **New** and select **Return Redirect**. The Add Return Redirect object dialog displays. Enter the secured URL for your OWA. Click **OK** to add the object and dismiss the dialog. The Set Action Object dialog re-displays. Click **OK** to set the object.
Click **Install Policy** to finish. Close the VPM.

Enable the HTTP service to intercept: Go to **Services > Proxy Services**.
Select the HTTP service and click **Edit**. The Edit Service dialog displays.

Select the `<All>` Listener and click **Edit**. The Edit Listener dialog displays.

Set the **Destination address** option to **Explicit** and the **Action** option to **Intercept**, leave the **Port range** option at 80. Click **OK**. The Edit Service dialog re-displays. Click **OK** to set and dismiss the dialog. Click **Apply** to finish.

Now, if your users enter "webmail.example.com" or "http://webmail.example.com," they are re-directed to "https://webmail.example.com."
Conclusion

The Blue Coat ProxySG provides an enterprise with greater security by front-ending access to an Outlook Web Access email server. The ProxySG acts as the termination point for HTTPS, offloading that service from the OWA server, and then forwarding the email requests to the OWA server for response. Additionally, an exception policy defined for user inactivity automatically logs the user off their session with the OWA server. This feature provides another level of security for users accessing email across public Web services and helps companies gain greater control of how their users access information using corporate resources.