Web Security Cloud

Configuring Proxy Chaining with the Forcepoint Cloud Service

Revision A

Contents

Introduction

Proxy chaining involves connecting two (or more) proxies together, with one proxy forwarding traffic to another. This configuration may be used if you have an existing proxy in your network that you wish to connect to Forcepoint Web Security Cloud. In this scenario, you can leave users' browser settings unchanged and configure your existing proxy to forward all HTTP, HTTPS, and FTP requests to Forcepoint Web Security Cloud.

- If your proxy is capable of using a PAC file, use the one provided in the Forcepoint Cloud Security Gateway Portal, also referred to as the cloud portal.

  This is ideal, because the Forcepoint Web Security Cloud PAC file changes automatically based on your policy settings.
- Otherwise, download a copy of the PAC file and duplicate its functionality within in your proxy configuration.

  In this case, you may have to make manual changes to your proxy configuration when your policy settings change.

Forcepoint Web Security Cloud has been tested with a number of commercially available proxies in chained proxy configuration. This document provides basic configuration instructions for the following third-party proxies, which have been tested and validated for use with the service:

- *Microsoft ISA Server or Forefront TMG*
- *Blue Coat ProxySG*
- *Squid Proxy*

Note

Proxy chaining is not applicable if you are deploying Forcepoint Web Security Cloud with an I Series appliance.

Related concepts

Microsoft ISA Server or Forefront TMG on page 3

Blue Coat ProxySG on page 8

Squid Proxy on page 12

Microsoft ISA Server or Forefront TMG

A Microsoft Internet Security and Acceleration (ISA) Server or Forefront Threat Management Gateway (TMG) server can be deployed as a downstream proxy with Forcepoint Web Security Cloud. You can configure proxy chaining in the following ways:

- **Basic chaining**: The ISA server does not perform any authentication before forwarding requests to the cloud proxy. The cloud proxy can perform manual authentication only.
- **NTLM pass-through**: The ISA server is aware of a requirement for NTLM identification but takes no part in the authentication, forwarding requests to the cloud proxy which then performs NTLM identification.
- **X-Authenticated-User**: The ISA server performs user authentication and forwards requests to the cloud proxy using the X-Authenticated-User header.

In this guide, “ISA/TMG” refers to ISA Server and Forefront TMG collectively. When instructions or information differ for the two products, they are referred to specifically as “ISA Server” or “Forefront TMG”.

Basic chaining

To set up your ISA/TMG server to chain with the upstream cloud proxy, follow the instructions below.

1) Log on to the ISA/TMG server and open the **Server Management** console.

2) Under **Configuration**, open the **Networks** option and select the **Web Chaining** tab. Under this tab a default rule is present. Leave this as it is.

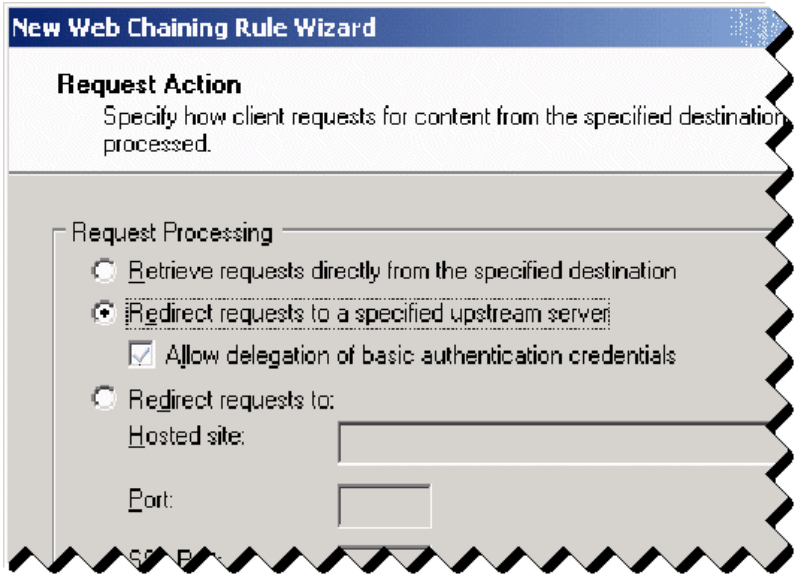
3) Click the **Tasks** tab, then click the **Create New Web Chaining Rule** link to start the wizard.

4) Give the rule a meaningful name such as Forcepoint Web Security Cloud, and click **Next**.

5) In the next section, choose the destinations to which this rule applies (in most cases, it applies to external networks).

6) Click **Add** and select the appropriate network.

7) Click **Next** to specify how requests are to be handled. This is where you specify that requests be sent to an upstream server (i.e., Forcepoint Web Security Cloud).



8) Select **Redirect requests to a specified upstream server** and click **Next**.

9) On the **Primary Routing** page, specify the address of the Forcepoint Web Security Cloud service: *webdefence.global.blackspider.com*

10) Specify port 8081 for both Port and SSL. Click **Next**.

11) On the **Backup Action** page, select the appropriate action for your organization. Your choice depends on whether you are willing to allow requests to be served directly, without using Forcepoint Web Security Cloud. Click **Next**.

12) Review your settings and click **Finish**.

Configuring exceptions

If there are any hosts that you do not want to use the proxy service, you must configure an exception for them. Minimally, you should add those hosts that are in the PAC file that is downloaded from the Forcepoint Web Security Cloud service (see Proxy auto-configuration (PAC) file in the Forcepoint Web Security Cloud help for more details).

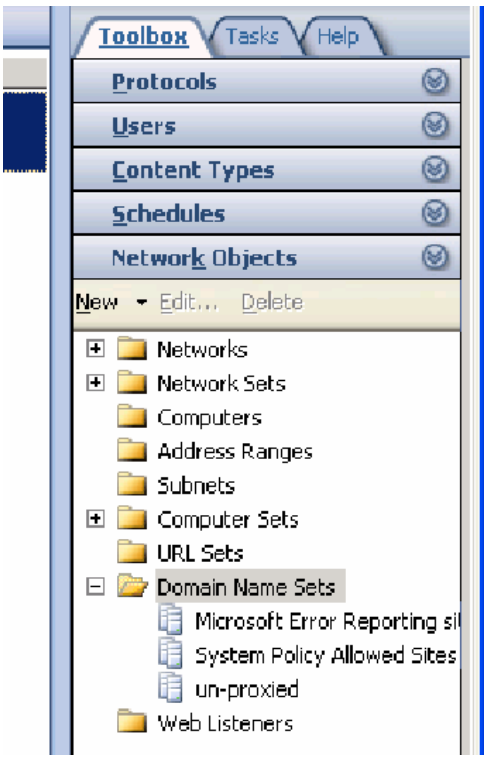
You should also configure direct access to the cloud portal to allow the following:

- Correct display of block pages
- End-user self-registration

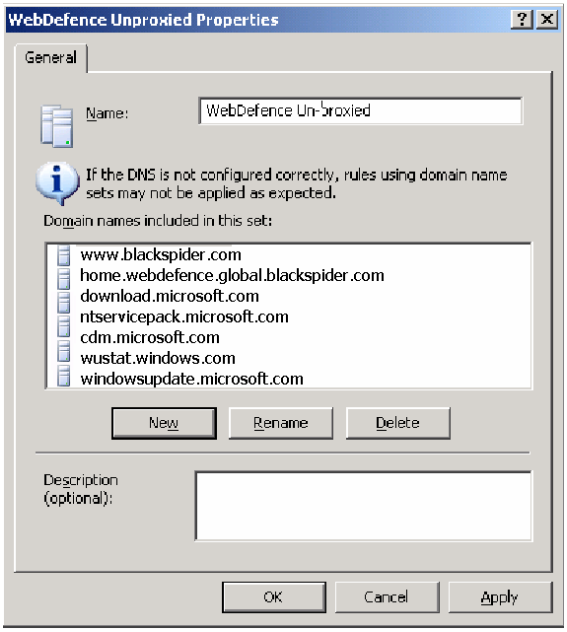
If you are using the roaming user home page, it should also be configured as an exception. The URL is:

```
http://home.webdefence.global.blackspider.com/
```

1) To configure exceptions, click **Firewall Policy**, then select **Network Objects** from the **Toolbox**.



2) Right-click **Domain Name Sets** and click **New Domain Name Set**.



3) Give the new set a name (e.g., Forcepoint Web Security Cloud Unproxied). In the **Domain names included in this set** section, add all Forcepoint Web Security Cloud global exceptions (from the Forcepoint Web Security Cloud PAC file). These include the following Microsoft Windows update sites:

```
download.microsoft.com
ntservicepack.microsoft.com
cdm.microsoft.com
wustat.windows.com
windowsupdate.microsoft.com
*.windowsupdate.microsoft.com
update.microsoft.com
*.update.microsoft.com
*.windowsupdate.com
```

Also, add the following cloud service sites:

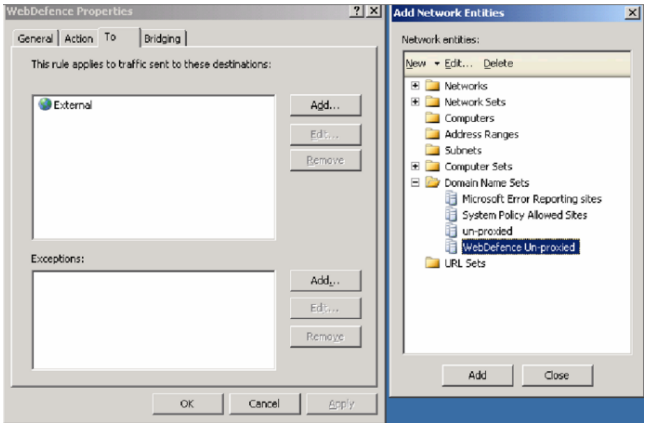
```
www.blackspider.com
mailcontrol.com
home.webdefence.global.blackspider.com
webdefence.global.blackspider.com
```

Include any other exceptions appropriate for your environment.

4) Click **OK** and **Apply** changes.

5) Navigate back to the proxy chaining policy you created above, open the policy and click the **To** tab.

6) In the **Exceptions** section, click **Add**.



7) Expand **Domain Name Sets**, select the domain set you just created (Forcepoint Web Security Cloud Unproxied), and click **Add**.

8) Click **Close** on **Add Network Entities**.

9) Click **OK** on the web chaining policy and **Apply** the changes.

Configuring NTLM pass through

To chain your ISA/TMG server with the cloud proxy and perform NTLM identification:

1) Follow the steps in *Basic chaining*.

2) Log on to the cloud portal.

3) Select **Web** > **Policy Management** > **Policies** > **policy name** > **Access Control**.

4) Select Authenticate users on first access, then select NTLM transparent identification where possible. For more information, see NTLM identification in the Web Security Cloud Help.

5) Click **Save**.

Related tasks
Basic chaining on page 3

Configuring X-Authenticated-User chaining

You can pass authentication details from your ISA/TMG server to the cloud proxy via a plug-in from Forcepoint LLC. This plug-in allows the cloud proxy to read the X-Forwarded-For and X-Authenticated-User headers sent by the downstream ISA/TMG server as part of a proxy chained configuration.

X-Forwarded-For	Contains the client IP address
X-Authenticated-User	When ISA authentication is turned on, this header will be populated with the user domain and username (domain\user).

With this setup, end users can be authenticated transparently by the cloud proxy, removing an authentication step and improving performance.

Two versions of the plug-in are available, for 32-bit ISA servers and 64-bit TMG servers. Zip files for both versions are available for download:

1) Log on to your Forcepoint website account.

2) Select the **Downloads** tab.

3) Select Forcepoint Web Security Cloud from the **Product** drop-down list.

4) In the list that appears, expand **TMG 64-bit plugin for Content Gateway or ISA 32-bit plugin for Content Gateway** to see the download details. You will need to scroll down to older product versions to see the ISA 32-bit plug-in. Click the download link to start the download.

Install the plug-in as follows:

1) Copy the appropriate `Websense-AuthForward.dll` file (for 32-bit or 64-bit) to the Microsoft ISA/TMG installation directory. The default directory for this file is `C:\Program Files\Microsoft ISA Server` for ISA server, or `C:\Program Files\Microsoft Forefront Threat Management Gateway` for ForefrontTMG.

For the 32-bit version, install the following files in the installation directory in addition to `Websense-AuthForward.dll`:

```
msvcp100.dll
msvcr100.dll
```

2) Open a Windows command prompt and change directory to the installation directory.

3) From the command prompt, type

```
regsvr32 Websense-AuthForward.dll
```

4) Verify the plug-in was registered in the ISA/TMG management user interface (**Start** > **Programs** > **Microsoft ISA Server** > **ISA Server Management**, or **Start** > **Programs** > **Microsoft Forefront TMG** > **Microsoft Forefront TMG Management**). In the Configuration (for 32-bit) or System (for 64-bit) section, select **Add-ins**, then click the **Web-filter** tab. The **WsAuthForward** plug-in should be listed.

To uninstall the plug-in, run the following command in a Windows command prompt from the ISA/TMG installation directory.

```
regsvr32 /u Websense-AuthForward.dll
```

Blue Coat ProxySG

Blue Coat ProxySG can be deployed as a downstream proxy with Forcepoint Web Security Cloud. You can configure proxy chaining in the following ways:

- **Basic chaining**: The Blue Coat server does not perform any authentication before forwarding requests to the cloud proxy. The cloud proxy can perform manual authentication only.
- **NTLM pass-through**: The Blue Coat server takes no part in authentication, forwarding requests to the cloud proxy which then performs NTLM identification.
- **X-Authenticated-User**: The Blue Coat server performs user authentication and forwards requests to the cloud proxy using the X-Authenticated-User header.

Basic chaining

In this case, Blue Coat ProxySG forwards requests to the cloud proxy but performs no authentication. End users can be authenticated using manual authentication only: prompting users for a user name and password the first time they access the Internet through a browser.

Use the Blue Coat Management Console to forward requests to the cloud proxy as follows:

1) In the **Blue Coat Management Console Configuration** tab, select **Forwarding** > **Forwarding Hosts**.

2) Select **Install from Text Editor** from the drop-down, and then click **Install**.

3) Update the Forwarding Hosts configuration file to point an alias name to webdefence.global.blackspider.com, port 8081. For example, if you choose the alias name **Forcepoint_Proxy**, enter the following at the end of the “Forwarding host configuration” section:

```
fwd_host Forcepoint_Proxy webdefence.global.blackspider.com
http=8081
```

4) Add the following to the end of the ‘Default fail-over sequence’ section:

```
sequence alias name
```

replacing *alias name* with the alias name that you chose in step 3.

5) When you have finished editing, click **Install**.

6) In the **Blue Coat Management Console Configuration** tab, click **Policy** and select **Visual Policy Manager**. Click **Launch**.

7) In the **Policy** menu, select **Add Forwarding Layer** and enter an appropriate policy name in the **Add New Layer** dialog box.

8) Select the **Forwarding Layer** tab that is created. The Source, Destination, and Service column entries should be **Any** (the default).

9) Right-click the area in the **Action** column, and select **Set**.

10) Select the alias name that you created (for example, Forcepoint_Proxy) from the list, and click **OK**.

11) Right-click the alias name in the Action column and select **Edit**.

12) Choose the forwarding behavior if your Blue Coat proxy cannot contact the cloud proxy: either to connect directly, or to refuse the browser request.

13) Click **OK**.

14) Click **Install Policy** in the **Blue Coat Visual Policy Manager**.

NTLM chaining

To chain Blue Coat ProxySG with the cloud proxy and perform NTLM identification:

1) Follow the steps in *Basic chaining, page 8*.

2) Log on to the cloud portal.

3) Go to the **Web** > **Policy Management** > **Policies** page, then select a policy.

4) Click the **Access Control** tab for the policy.

5) Select **Always authenticate users on first access**, then select **NTLM transparent identification where possible**. For more information, see NTLM identification in the cloud portal Help.

6) Click **Save**.

X-Authenticated-User chaining

You can pass authentication details from your Blue Coat proxy to send X-Forwarded-For and X-Authenticated-User headers to the cloud proxy either by manually editing a policy text file, or defining the policy in Blue Coat Visual Policy Manager.

X-Forwarded-For	Contains the client IP address
X-Authenticated-User	When Blue Coat authentication is turned on, this header will be populated with the user domain and username (domain\user).

With this setup, end users can be authenticated transparently by the cloud proxy, removing an authentication step and improving performance.

Note that for Blue Coat to service HTTPS requests properly with the following setup, you must have a Blue Coat SSL license and hardware card.

Editing the local policy file

In the Blue Coat Management Console **Configuration** tab, click **Policy** in the left column and select **Policy Files**. Enter the following code in the current policy text file, using an Install Policy option:

```
<Proxy>
action.Add[header name for authenticated user](yes)

define action dd[header name for authenticated user]
set(request.x_header.X-Authenticated-User, "WinNT://
$(user.domain)/$(user.name)")
end action Add[header name for authenticated user]

action.Add[header name for client IP](yes)

define action dd[header name for client IP]
set(request.x_header.X-Forwarded-For,$(x-client-address))
end action Add[header name for client IP]
```

Using the Blue Coat graphical Visual Policy Manager

Before you configure the Blue Coat header policy, ensure that NTLM authentication is specified in the Blue Coat Visual Policy Manager (**Authentication** > **Windows SSO**). Set Forcepoint Web Security Cloud as the forwarding host (in the Blue Coat Management Console **Configuration** tab, **Forwarding** > **Forwarding Hosts**). The address of the Forcepoint Web Security Cloud service is webdefence.global.blackspider.com, port 8081.

In the Blue Coat Management Console **Configuration** tab, click **Policy** and select **Visual Policy Manager**. Click **Launch** and configure the header policy as follows:

1) In the **Policy** menu, select **Add Web Access Layer** and enter an appropriate policy name in the **Add New Layer** dialog box.

2) Select the **Web Access Layer** tab that is created.

3) The Source, Destination, Service, and Time column entries should be **Any**(the default).

4) Right-click the area in the **Action** column, and select **Set**.

5) Click **New** in the Set Action Object dialog box and select **Control Request Header** from the menu.

6) In the **Add Control Request Header Object** dialog box, enter a name for the client IP Action object in the **Name** entry field.

7) Enter **X-Forwarded-For** in the Header Name entry field.

8) Select the **Set value** radio button and enter the following value:

```
$(x-client-address)
```

9) Click **OK**.

10) Click **New** and select **Control Request Header** again.

11) In the **Add Control Request Header Object** dialog box, enter a name for the authenticated user information Action object in the Name entry field.

12) Enter **X-Authenticated-User** in the Header Name entry field.

13) Select the **Set value** radio button and enter the following value:

```
WinNT://$(user.domain)/$(user.name)
```

14) Click **OK**.

15) Click **New** and select **Combined Action Object** from the menu.

16) In the **Add Combined Action Object** dialog box, enter a name for a proxy chain header in the Name entry field.

17) In the left pane, select the previously created control request headers and click **Add**.

18) Select the combined action item in the **Set Action Object dialog** box and click **OK**.

Click **Install Policy** in the Blue Coat Visual Policy Manager.

Squid Proxy

Forcepoint Web Security Cloud supports the configuration of a chained Squid open source downstream proxy, in the following cases:

- Basic chaining
- For policies where NTLM is enabled and end users are asked to authenticate for Forcepoint Web Security Cloud

The Squid proxy must be version 3.1.5 or later.

Basic chaining

In this case, Squid forwards requests to the cloud proxy but performs no authentication. End users can be authenticated using manual authentication only: prompting users for a user name and password the first time they access the Internet through a browser.

Configure Squid to forward requests to the cloud proxy as follows:

1) Define one or more ACLs to identify sites that should be not be filtered through Forcepoint Web Security Cloud. These must include certain service-specific sites, and should include any other sites that are not normally handled through the cloud service. You can identify these sites by examining the service-generated PAC file available at http://pac.webdefence.global.blackspider.com:8082/proxy.pac.
   You should also configure direct access to the cloud portal to allow the following:
   - Correct display of block pages
   - End-user self-registration

   The roaming user home page, if used, should also be configured as an ACL.

   The following sites **must** be included in the ACLs:

   ```
   acl WBSN dstdomain .mailcontrol.com
   acl WBSN dstdomain www.blackspider.com
   acl WBSN dstdomain webdefence.global.blackspider.com
   always_direct allow WBSN
   ```

2) Force all other sites to use the cloud proxy as follows:

   ```
   never_direct allow all
   ```

3) Tell Squid the location of the upstream cloud proxy:

   ```
   cache_peer webdefence.global.blackspider.com parent 8081 0
   no-query default no-digest
   ```

NTLM chaining

The Squid proxy performs local NTLM identification, then forwards the appropriate Proxy-Authorization headers as an NTLM Type 3 message to the cloud proxy for further transparent user authentication. Squid can maintain multiple connections to the cloud proxy, allowing the sharing of connections across users but ensuring that each

request is associated with the correct user. When Squid reassigns a connection to another user, only then is a new Proxy-Authorization header sent for that user.

To use this setup, configure Squid to do the following:

1) Perform NTLM authentication.

2) Forward requests to the cloud proxy.

3) Forward user information to the cloud proxy.

Configuring Squid for NTLM authentication

To configure Squid to perform NTLM authentication of users, refer to the Squid documentation.

Forwarding requests to the cloud proxy

To configure Squid to forward requests to the cloud proxy:

1) Define one or more ACLs to identify sites that should be not be filtered through Forcepoint Web Security Cloud. These must include certain service-specific sites, and should include any other sites that are not normally handled through the cloud service. You can identify these sites by examining the service-generated PAC file available at http://pac.webdefence.global.blackspider.com:8082/proxy.pac.
   The following sites **must** be included in the ACLs:

```
acl WBSN dstdomain .mailcontrol.com
acl WBSN dstdomain www.blackspider.com
acl WBSN dstdomain webdefence.global.blackspider.com
always_direct allow WBSN
```

2) Force all other sites to use the cloud proxy as follows:

```
never_direct allow all
```

3) Tell Squid the location of the upstream cloud proxy:

```
cache_peer webdefence.global.blackspider.com parent 8081 0
no-query default no-digest
```

Forwarding user information to the cloud proxy

To configure squid to forward user information, add option login=PASS to the cache-peer line:

```
cache_peer webdefence.global.blackspider.com parent 8081 0
no-query default no-digest login=PASS
```

Published 08 August 2024