Forcepoint

Web Security Cloud

Firewall Redirect: Forwarding Traffic to the Forcepoint Cloud Service

Revision A

Contents

Introduction

Firewall redirection is a simple and effective method for sending web traffic to the cloud service. Firewall redirection is easy to configure and maintain, with no configuration required on client machines - traffic is redirected transparently. Firewall redirection works for both HTTP and HTTPS traffic. NTLM and basic authentication are supported.

Firewall redirection is well suited for:

- Guest Wi-Fi networks where users do not belong to a domain, and authentication and SSL decryption are not required.
- Branch offices in hybrid deployments (where no on-premises appliance is installed).
- Other deployments where the Forcepoint Web Security Endpoint client or proxy auto-config (PAC) files cannot be used - for example, where there are unmanaged devices that require web enforcement.

Important

Cloud service firewall redirection does not provide automatic data center failover. Where transparent redirection with automatic failover is required, please use Forcepoint GRE or IPsec connectivity.

This document includes the following topics:

- Supported devices
- Configuration for firewall redirection
- Device configuration examples
- Cloud service IP addresses
- Configuring end-user authentication with firewall redirect
- Configuring proxy bypass destinations with firewall redirect
- Limitations and known issues

Related concepts
Supported devices on page 3
Configuration for firewall redirection on page 3
Device configuration examples on page 4
Configuring proxy bypass destinations with firewall redirect on page 7
Limitations and known issues on page 8
Cloud service IP addresses on page 4

Related tasks
Configuring end-user authentication with firewall redirect on page 5

Supported devices

The following devices have been tested and verified to support firewall redirection to the Forcepoint cloud service:

- Forcepoint NGFW (port 80, 443)
- Aruba Networks (ports 80, 443)
- Check Point Enterprise Firewall (ports 80, 443)
- Cisco ASA (ports 80, 443)
- Juniper SSG (ports 80, 443)
- Juniper SRX (ports 80, 443)
- SonicWall (port 80 only)

Note

Cisco ISR and Palo Alto devices do not support firewall redirection to the Forcepoint cloud service.

Configuration for firewall redirection

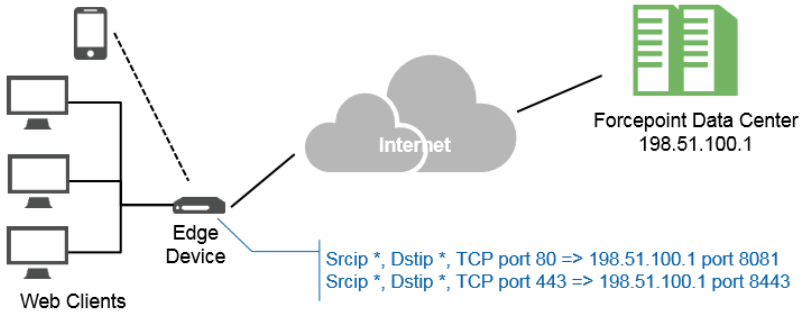
The requirements for using firewall redirect are as follows:

- All web traffic must exit your network through an edge device (such as a supported firewall or router).
- Port forwarding (NAT and PAT) must be configured on the edge device to forward web traffic on ports 80 and 443 to specific Forcepoint data center IP addresses and ports:
  - Forward port 80 (HTTP) traffic to port 8081
  - Forward port 443 (HTTPS) traffic to port 8443
  - Different IP addresses must be used, per data center, for cloud and hybrid configurations. See *Cloud service IP addresses*.

Note

When using Forcepoint NGFW for firewall redirection to the cloud service in Generic Proxy mode, use port 8081 as the destination port for both HTTP and HTTPS.

The following diagram shows an edge device redirecting traffic to a Forcepoint data center. Port 80 (HTTP) traffic is forwarded to port 8081, while port 443 (HTTPS) traffic is forwarded to port 8443. Traffic is forwarded to the IP address of the geographically closest data center.



Related concepts

Cloud service IP addresses on page 4

Preventing data leakage

As a best practice, Forcepoint recommends that you lock down your firewall to prevent traffic leakage via different protocols and ports. In particular, Google Chrome can default to the experimental QUIC protocol, which uses UDP on port 443. We recommend that you block UDP traffic on port 443 in order to force traffic over TCP. For more information, see the Knowledge Base article Google QUIC protocol is not supported by the Forcepoint cloud service.

Device configuration examples

Detailed configuration examples for the following devices can be found in the Forcepoint Knowledge Base:

- Aruba
- Check Point
- Cisco ASA
- Juniper SSG
- SonicWall

You must be logged in to My Account to see these articles. To create a customer account, navigate to the Customer Hub Home page, and then click the **Create Account** link.

Cloud service IP addresses

To locate the nearest cloud data center, refer to the following article in the Forcepoint Knowledge Base, which contains a list of the Forcepoint cloud service data centers and their locations: Cloud service data center IP addresses and port numbers.

To forward traffic to a particular data center:

1) Use the article above to determine the appropriate country and city, as well as the data center name (usually a single letter or short code).

2) Perform a DNS lookup using a data center-specific DNS name in the following format:

```
cluster.NAME.SERVICE.global.blackspider.com
```

Where NAME is the letter or code for the data center, and SERVICE indicates either cloud (“webdefence”) or hybrid (“hybrid-web”).

This returns the service IP address for the specified cluster. For example:

- Cloud (webdefence):

```
$ nslookup cluster.x.webdefence.global.blackspider.com
Name: cluster.x.webdefence.global.blackspider.com
Address: 85.115.33.180
$ nslookup cluster.g.webdefence.global.blackspider.com
Name: cluster.g.webdefence.global.blackspider.com
Address: 208.87.233.180
```

- Hybrid (hybrid-web):

```
$ nslookup cluster.x.hybrid-web.global.blackspider.com
Name: cluster.x.hybrid-web.global.blackspider.com
Address: 85.115.33.150
```

DNS lookup

You can also locate the nearest cloud data center by performing a DNS lookup from your network. Use the following lookups for cloud and hybrid deployments:

- Cloud:

```
nslookup webdefence.global.blackspider.com
```

- Hybrid:

```
nslookup hybrid-web.global.blackspider.com
```

Note

The result of this DNS lookup depends on your DNS configuration, and may not always return the most appropriate data center. Verify the IP destination returned by referring to the article above.

Configuring end-user authentication with firewall redirect

Two types of user authentication are supported for firewall redirect: NTLM and basic authentication.

- NTLM identification is seamless, and uses the end user’s NTLM credentials to identify them to the service.

- Basic (manual) authentication uses the end user's email address and password. Users receive an authentication prompt when they attempt to navigate to a website.

Note

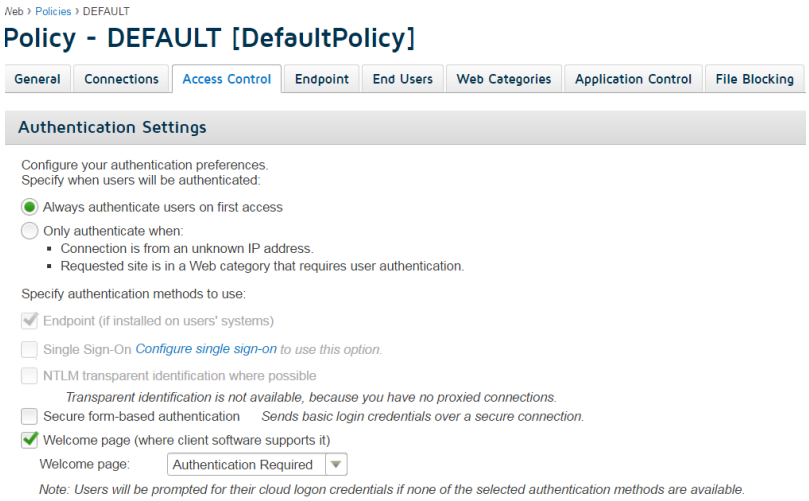
Authentication is an account-level setting which is applied to all users. You cannot disable authentication for one set of users (for example, on a guest network), while enabling it for others.

To enable authentication:

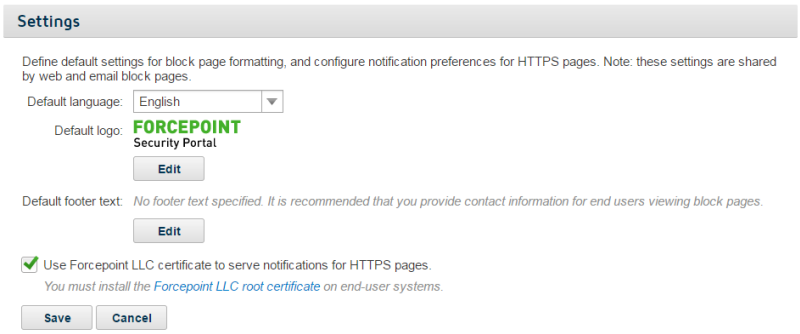
Steps

1) Navigate to the **Web** > **Policies** page in the cloud portal and select a policy.

2) Select the **Access Control** tab for the policy, and select **Always authenticate users on the first access**.



3) If you are using SSL decryption, also navigate to the **Web** > **Block & Notification Pages** page and mark the **Use Forcepoint LLC certificate to serve...** check box. You must also install the Forcepoint root certificate on all end user machines in your environment to enable SSL decryption and allow the authentication page and block pages to be displayed for HTTPS sites.



If this setting is **not** enabled:

- Users accessing HTTPS sites are allowed to browse anonymously.
- When a user navigates to a blocked URL, the connection is closed, with no block page displayed.

4) Add the following URLs to the local intranet zone in users' browsers:

```
http://proxy-login.blackspider.com
https://ssl-proxy-login.blackspider.com
```

You must add the URL proxy-login.blackspider.com to the registry locations listed below to ensure that this site is excluded from the Chrome https upgrades:

- Registry key for Edge: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\HttpAllowlist`
- Registry key for Chrome: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\HttpAllowlist`

For information on how to do this for various browsers, see the knowledge base article Configuring browsers for NTLM identification.

Configuring proxy bypass destinations with firewall redirect

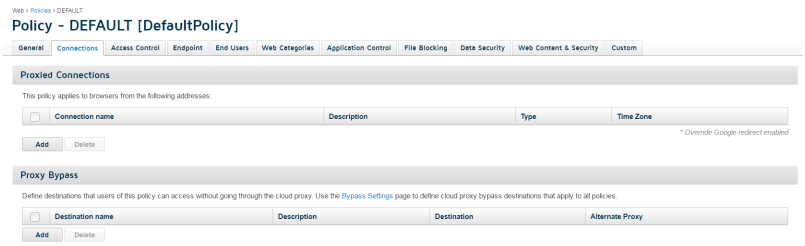
You can configure the cloud service to allow users to access some domains without policy enforcement. These are called proxy **bypass destinations**. Define proxy bypass destinations in any of the following ways. (For more detailed instructions, see the Forcepoint Web Security Cloud Help).

- To configure bypass destinations within individual policies:

  1) Navigate to **Web** > **Policies** and select a policy.

  2) Click the **Connections** tab.

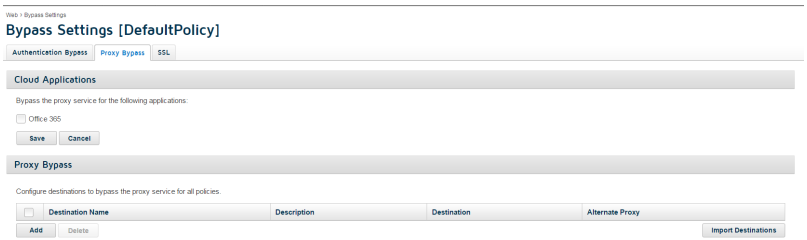
  3) In the **Proxy Bypass** section, click **Add**.
  These bypass destinations affect only users assigned to the specified policy.



- To configure domains that will be bypassed at the account level:

  1) Navigate to **Web** > **Bypass Settings**.

  2) In the **Proxy Bypass** section, click **Add**.
  These bypass destinations affect all end users in the account, regardless of which policy they are assigned.



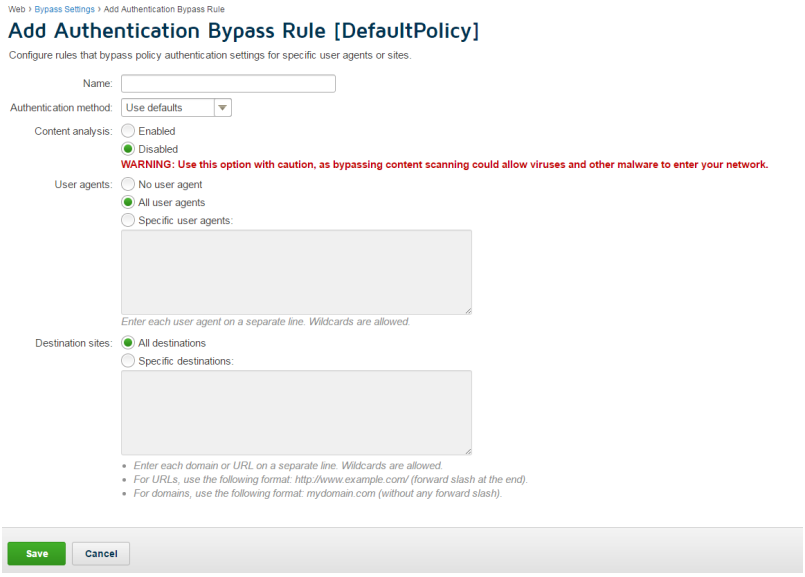
- To configure the domains via the “User Agent & Destinations” bypass list with content analysis disabled:

  1) Navigate to **Web** > **Bypass Settings**.

  2) In the **User Agent & Destinations** section, click **Add**.

Note

If you are using PAC files to direct traffic to the service, use this method if you do not want to add the bypassed domains to the policy PAC file.



In all of these cases, traffic is forwarded to the cloud service, but no policy enforcement occurs. The cloud service transparently forwards the traffic upstream. These transactions are logged in reporting with a bypass action.

Note

Forcepoint Cloud Operations may block some domains at their discretion, if traffic to those domains is known to cause problems. If this occurs, all traffic to these domains is blocked, and it is not possible to send this traffic through the cloud service, regardless of your bypass settings.

Limitations and known issues

The following items are the known limitations of using this method to direct traffic to the cloud service.

- Certain websites might redirect from a single URL to multiple domains. This causes multiple redirects to **proxy-login.blackspider.com** for authentication, which may result in the number of redirects exceeding the

browser redirect limit. If this occurs, the browser may display a “too many redirects” or “redirection loop” error page. As a workaround, administrators can increase the redirect limit for Firefox and Internet Explorer, or users can refresh the page. See *Increasing the browser redirection limit*, for more information.

- The **acceptable use policy button** is not enabled in environments that use firewall redirect. This will be addressed in a future release.
- When user authentication is enabled in a policy, decryption bypass is not possible, and SSL decryption bypass settings are ignored. It is, however, still possible to do authentication decryption bypass, which causes requests to be processed anonymously.
- As internal IP addresses are not visible in deployments that use firewall redirect, authentication bypass based on internal IP address is not available. Likewise, policy enforcement based on internal IP address is not supported.
- When using firewall redirection, Dropbox is not supported for use with the Protected Cloud Apps feature in Forcepoint Web Security Cloud.
- Firewall redirect does not support automatic data center failover. This is planned for a future release. Where transparent redirection with automatic failover is required, please use the Forcepoint GRE or IPsec service.
- SNI is required for HTTPS traffic when using transparent proxy.
  - Windows XP does not support SNI and is, therefore, not supported for Forcepoint Firewall redirect.
  - Encrypted Client Hello (aka Encrypted SNI) is not supported when using transparent proxy.

Related concepts

Increasing the browser redirection limit on page 9

Increasing the browser redirection limit

You may want to increase the redirection limit of users’ browsers because certain websites might redirect from a single URL to multiple domains. This causes multiple redirects to proxy-login.blackspider.com for authentication, which can result in the number of redirects exceeding the browser redirect limit. If this occurs, the browser may display a “too many redirects” or “redirection loop” error page. This section describes how to increase the browser redirection limit for Internet Explorer and Firefox.

Note

Google Chrome has a maximum redirect limit of 20, which cannot be changed.

Internet Explorer

The screenshots in this section are taken from the Microsoft Registry Editor in Windows 7.

Changing the redirection limit for Internet Explorer requires changes to the Windows Registry. Proceed with caution.

Warning

Errors in the Windows Registry can cause serious problems, including rendering the system unusable. Always back up the Windows Registry before making changes.

Steps

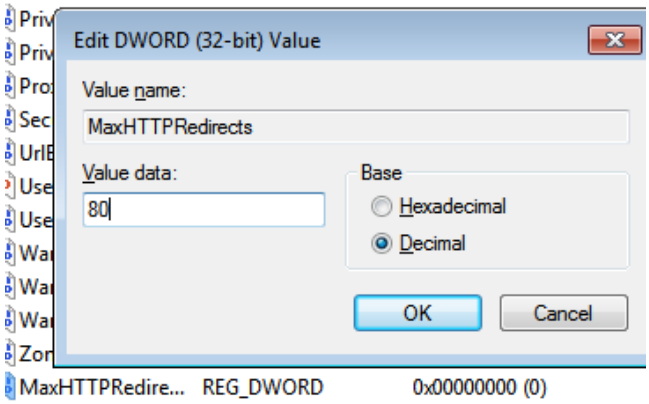
1) Open the Windows Registry (**Start** > **cmd** > **regedit**).

2) Navigate to the following location:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

3) Right-click the folder and select **New**, then and select **DWORD (32 bit)**.

4) Rename the DWORD value to **MaxHttpRedirects** and modify the DWORD to decimal **80**.



5) Click **OK**.

Firefox

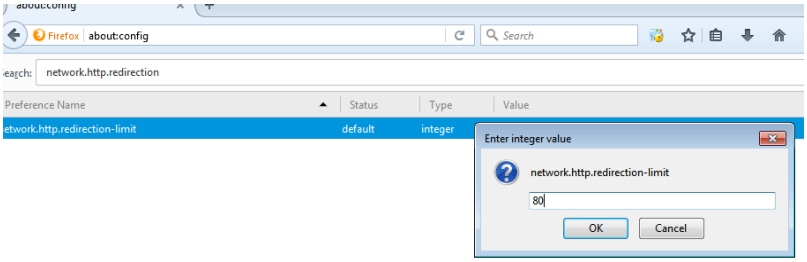
The screenshots in this section are taken from Mozilla Firefox version 40. Use the Firefox configuration editor to update the redirection limit:

Steps

1) Launch Firefox and type **about:config** in the address bar.

2) Search for **network.http.redirection-limit** and double click it.

3) Change the value to **80**.



4) Click **OK**.

Published 08 August 2024