



Next Generation Firewall

6.1 and higher

**How to forward web traffic
to Forcepoint Web Security Cloud**

Contents

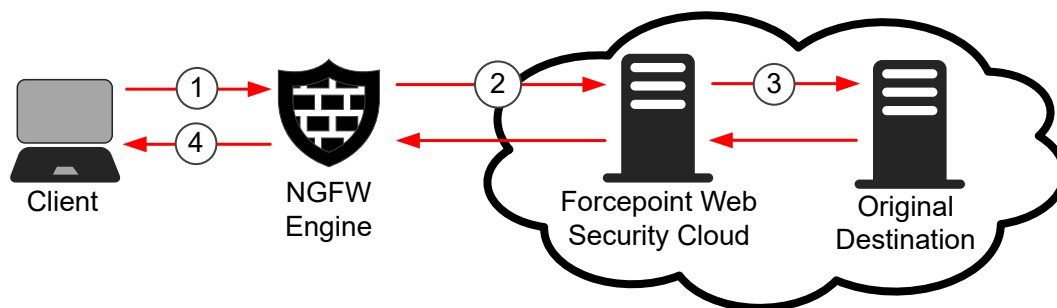
- [Introduction](#) on page 2
- [Supported methods](#) on page 3
- [About EasyConnect](#) on page 5
- [Using Access rules](#) on page 11
- [Using NAT rules](#) on page 12
- [Using a custom Service element](#) on page 14
- [Using a policy-based VPN](#) on page 17

Introduction

Forcepoint Next Generation Firewall (Forcepoint NGFW) can forward web traffic to Forcepoint Web Security Cloud for inspection. The traffic is inspected in Web Security Cloud and transparently forwarded to the destination.

You must have a subscription to use the Web Security Cloud service. The service's data centers are geographically distributed. The NGFW Engine uses DNS resolution to select the IP address of the geographically closest data center. Both Windows Challenge/Response (NTLM) authentication and manual authentication using an email address and password are supported in Web Security Cloud.

How forwarding web traffic works



- 1 Traffic from the client arrives at the NGFW Engine (a Single Firewall or a Firewall Cluster).
- 2 Access rules or NAT rules in the Firewall policy determine which connections are forwarded to Web Security Cloud.
- 3 Web Security Cloud inspects the traffic, then forwards it to the original destination.
- 4 Web Security Cloud inspects the reply packets from the server, then forwards them to the client.

For more information, see the following documentation at <https://support.forcepoint.com/Documentation>.

- *Forcepoint Next Generation Firewall Product Guide*
- *Forcepoint Web Security Cloud Getting Started Guide*
- *Security Portal Help*

Supported methods

Select the method to use based on your needs and the Forcepoint NGFW version.

There are configuration steps in both Web Security Cloud and the Forcepoint NGFW Security Management Center (SMC). Use the cloud Security Portal to configure Web Security Cloud, and the Management Client component of the SMC (SMC Management Client) to configure the SMC.



Note

Different methods for forwarding traffic from the Forcepoint NGFW to Web Security Cloud require specific Forcepoint NGFW and SMC versions. The SMC version must be the same major version or higher than the Forcepoint NGFW version.

Access rules



Note

This method requires Forcepoint NGFW version 6.6.3 or higher and SMC 6.6.2 or higher.

- 1) In Web Security Cloud, configure an EasyConnect service.
- 2) In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.
- 3) In the Action options of an Access rule, select the Proxy Server to forward traffic to.

We recommend that you use Access rules to forward traffic. However, if you have a more complex environment and existing NAT rules, forward traffic using the NAT rules method instead. When you use Access rules to forward traffic, all existing NAT rules in the policy are ignored, but element-based NAT is taken into account. All destination NAT definitions are ignored. If element-based source NAT definitions have been defined and if default NAT has been enabled in the properties of the NGFW Engine, those NAT definitions are processed.

Element-based NAT is sufficient in most cases, but if you need to use NAT rules to have greater flexibility, you must forward traffic using the NAT rules method.

NAT rules



Note

This method requires Forcepoint NGFW version 6.5 or higher.

Use this method if you have existing NAT rules for a more complex NAT setup. Use NAT rules if you want to, for example, forward traffic while using Outbound Multi-Link elements to select the network link for the traffic.

- 1) In Web Security Cloud, configure an EasyConnect service.
- 2) In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.
- 3) In the NAT options of a NAT rule, select the Proxy Server to forward traffic to.

Custom Service element



Note

This method requires Forcepoint NGFW version 6.4 or higher.

- 1) In Web Security Cloud, configure an EasyConnect service.
- 2) In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.
- 3) Create a custom Service element that references the Proxy Server.
- 4) Use the custom Service element in Access rules.

Policy-based VPN



Note

This method requires SMC version 6.1 or higher.

- 1) In the cloud Security Portal, configure Forcepoint Web Security Cloud to receive traffic from the NGFW Engine. Add the Forcepoint NGFW Engine as an Edge Device using the IPsec Advanced feature of Web Security Cloud.
- 2) In the SMC Management Client, import predefined VPN elements to create a policy-based VPN.
- 3) Add an access rule to redirect traffic into the VPN.

Related concepts

[Using Access rules](#) on page 11

[Using NAT rules](#) on page 12

[Using a custom Service element](#) on page 14

[Using a policy-based VPN](#) on page 17

About EasyConnect

When using the Access rules, NAT rules, or custom Service element method, you must configure an EasyConnect service in the cloud Security Portal for Web Security Cloud and create a Proxy Server element in the SMC Management Client.

Using key IDs

It can take up to an hour for a password change to be fully propagated in Web Security Cloud. To avoid downtime when updating the password, there are multiple passwords that are automatically generated in Web Security Cloud, and each password has a key ID assigned.

See the following example of use:

- 1) In the SMC Management Client, three NGFW Engines are configured to use key ID 1. The password for key ID 1 is 123xxxxxx.
- 2) In Web Security Cloud, an additional password (321yyyyyy) is assigned to key ID 2.
- 3) One by one, the SMC administrator configures the three NGFW Engines to use key ID 2. Because both key ID 1 and key ID 2 can be used to access Web Security Cloud, there is no downtime.
- 4) When all the NGFW Engines have been configured to use key ID 2, the Web Security Cloud administrator can regenerate the password for key ID 1 in Web Security Cloud.

Configure an EasyConnect service in the cloud Security Portal

You must configure an EasyConnect service for Forcepoint Web Security Cloud to accept connections from the NGFW Engine.

For more information, see the *Security Portal Help* at <https://support.forcepoint.com/Documentation>.

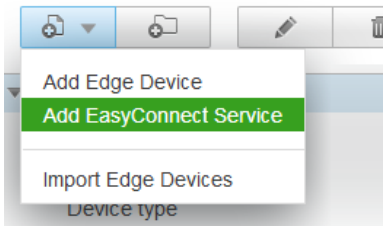
Steps

- 1) Log on to the cloud Security Portal at <https://admin.forcepoint.net/portal>.
- 2) Browse to **Web > Device Management**.

- 3) Select  **Add > Add EasyConnect Service**.

Web > Device Management

Device Management



- 4) Enter a name and a description.
- 5) To open a view that shows the customer ID and password that you need when creating the Proxy Server element in the SMC Management Client, click the **Connectivity Details** text link.
- 6) Click **Save**.

Next steps


In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.



Create a Proxy Server element that represents Web Security Cloud

In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.

Before you begin

Configure an EasyConnect service in the cloud Security Portal, and note the customer ID and password.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**, then browse to **Network Elements**.
- 2) Browse to **Servers**.
- 3) Select  **New > Proxy Server**.
- 4) Configure the settings.
- 5) In the **Address** field, enter `webdefence.global.blackspider.com`.

- 6) From the **Balancing Mode** drop-down list, select **First Available Server**.
The first IP address listed or resolved by DNS is used by default.
- 7) On the **Services** tab, enter 8090 as the port in the **Proxy Service Listening Port** field.
This is the port for HTTP connections.
- 8) Select **HTTPS**, then enter 8011 as the port.
- 9) From the **Proxy Service** drop-down list, select **Forcepoint Web Security Cloud**.
- 10) In the **Customer ID** field, enter the customer ID for the service.
Get the customer ID from the cloud Security Portal.
- 11) Select which key to use from the **Key ID** drop-down list, then enter the password for that key in the **Password** field.
Get the password from the cloud Security Portal.
- 12) Click **OK**.

Next steps

- If you are using the Directory Synchronization Tool to synchronize users with Web Security Cloud, verify that the name of the External LDAP Domain element matches the Windows logon domain.
- Do the following, depending on the method you want to use:
 - Access rules method — Add the Access rule to the policy of the NGFW Engine.
 - NAT rules method — Add the NAT rule to the policy of the NGFW Engine.
 - Custom Service element method — Create the Service element.

Related concepts

[Using Access rules](#) on page 11


[Using NAT rules](#) on page 12

[Using a custom Service element](#) on page 14

Verify the name of the LDAP domain

If you use the Directory Synchronization Tool to synchronize users with Web Security Cloud, verify that the name of the External LDAP Domain element in the SMC Management Client is the same as the name of the Windows logon domain.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**, then browse to **User Authentication**.
- 2) Select **Users** to view the list of configured LDAP domains.

- 3) Right-click the External LDAP Domain element that represents the Windows logon domain, then select **Properties**.
- 4) Verify that the name of the External LDAP Domain element matches the name of the Windows logon domain.

Next steps

If the name of the External LDAP Domain element matches the name of the Windows logon domain, no further actions are needed.

If the name does not match, do the following depending on the SMC version:

- SMC 6.6.3 or higher — Rename the External LDAP Domain element to match the name of the Windows logon domain, then continue the EasyConnect configuration according to the preferred method.
- SMC 6.6.2 or lower — Create a new External LDAP Domain element, then update the references to user groups and users in the policy of the NGFW Engine.

Create a new LDAP domain

If the name of the External LDAP Domain element does not match the name of the Windows logon domain, you must create a new External LDAP Domain element, then update the references to user groups and users in the policy of the NGFW Engine.



Note

This task is only required if you use SMC 6.6.2 or lower.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Configuration**, then browse to **User Authentication**.
- 2) Right-click **Users**, then select **New > External LDAP Domain**.
- 3) Enter the name of the Windows logon domain as the name of the External LDAP Domain element.
- 4) Select **Default LDAP Domain**.
The default LDAP domain is used for all authentication unless otherwise specified in the IPv4 or IPv6 Access rules.
- 5) Select a server, then click **Add** to bind the LDAP Server to the LDAP domain.
- 6) (Optional) On the **Default Authentication** tab, click **Select** to define the allowed authentication methods for all accounts in this LDAP domain.
- 7) Click **OK**.
The new External LDAP Domain element is added to the list of available LDAP domains.

Next steps

Update the references to users in the policy of the NGFW Engine to refer to user groups and users that belong to the new LDAP domain.

Update references to users in the policy

If you have created a new External LDAP Domain element for EasyConnect, replace the references to user groups and users that belong to the old LDAP domain with references to user groups and users that belong to the new LDAP domain in the policy of the NGFW Engine.

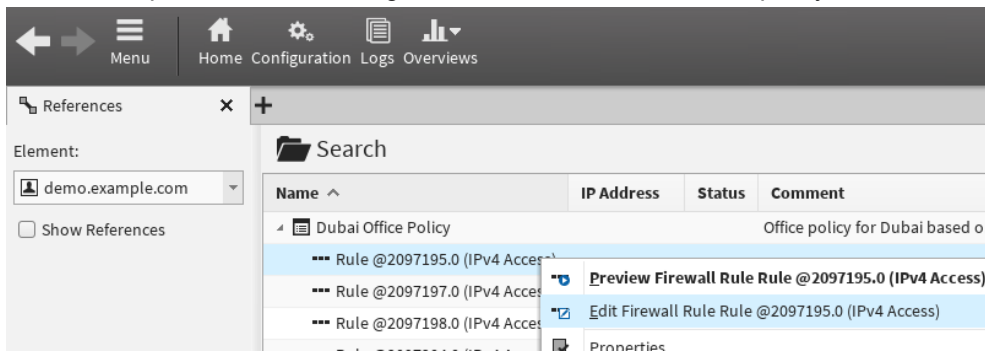


Note

This task is only required if you use SMC 6.6.2 or lower.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Configuration**, then browse to **User Authentication**.
- 2) Right-click the name of the old External LDAP Domain element, then select **Tools > Where Used?**.
A list of policies and rules that contain references to user groups and users associated with the LDAP domain is shown.
- 3) Click the arrow in front of the name of each policy to view the list of rules that contain references to user groups and users.
- 4) In the list of policies and rules, right-click the first rule in the first policy, then select **Edit <name of rule>**.



The policy opens with the rule highlighted.


- 5) Add a copy of the existing rule in the policy.
 - a) Right-click the rule, then select **Rule > Copy Rule**.
 - b) Right-click the rule, then select **Paste**.
A copy of the rule is added in the policy.
- 6) Update the references to user groups and users in the new rule that you added.
 - a) Remove the current user groups and users from the new rule.

- b) In the **Resources** pane, select **Users**, then select the new LDAP domain.
 - c) Drag and drop the user groups and users to the new rule.
- 7) Right-click the rule that contains references to the user groups and users that belong to the old LDAP domain, then select **Disable**.



Tip

You can remove this rule later when you have confirmed that user groups and users that belong to the new LDAP domain work correctly in the new rule that you added.

- 8) If other rules that belong to the same policy contain references to user groups or users that belong to the old LDAP domain, open each rule for editing, create a new rule with references to user groups and users in the new LDAP domain, then disable the old rule.
- 9) When you have updated all the references to user groups and users that belong to the old LDAP domain, click  **Save and Install**.
- 10) If there are references to user groups and users that belong to the old LDAP domain in rules in any other policies, remove the references to them in the same way.
- 11) (Recommended) When you have removed all the references to user groups and users that belong to the old LDAP domain from all the policies, right-click the old External LDAP Domain element, then select **Delete**.
- If any references to user groups and users in the LDAP domain still remain, a list of the references is shown. You must remove all the remaining references before you can remove the External LDAP Domain element.

Next steps

Do the following, depending on the method you want to use:

- Access rules method — Add the Access rule to the policy of the NGFW Engine.
- NAT rules method — Add the NAT rule to the policy of the NGFW Engine.
- Custom Service element method — Create the Service element.

Related concepts

[Using Access rules](#) on page 11

[Using NAT rules](#) on page 12

[Using a custom Service element](#) on page 14

Using Access rules

You can use Access rules to forward traffic that uses the HTTP and TLS Network Applications to Forcepoint Web Security Cloud.



Note

This method requires Forcepoint NGFW version 6.6.3 or higher and SMC 6.6.2 or higher.

Follow these general steps:

- 1) Configure an EasyConnect service in the cloud Security Portal.
- 2) In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.
- 3) Define the Access rule that selects traffic for forwarding to Web Security Cloud.

NAT considerations when using Access rules

We recommend that you use Access rules to forward traffic. However, if you have a more complex environment and existing NAT rules, forward traffic using the NAT rules method instead. When you use Access rules to forward traffic, all existing NAT rules in the policy are ignored, but element-based NAT is taken into account. All destination NAT definitions are ignored. If element-based source NAT definitions have been defined and if default NAT has been enabled in the properties of the NGFW Engine, those NAT definitions are processed.

Element-based NAT is sufficient in most cases, but if you need to use NAT rules to have greater flexibility, you must forward traffic using the NAT rules method. Use NAT rules if you want to, for example, forward traffic while using Outbound Multi-Link elements to select the network link for the traffic.

Related tasks

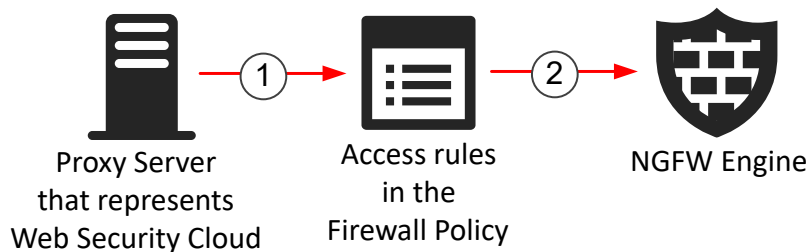
[Configure an EasyConnect service in the cloud Security Portal](#) on page 5

[Create a Proxy Server element that represents Web Security Cloud](#) on page 6

[Add an Access rule to forward traffic](#) on page 12

Elements used when using Access rules

The following elements are used when using Access rules to forward web traffic to Web Security Cloud.



1 The Proxy Server element is referenced in the Access rules in the Firewall Policy.


2 The Firewall Policy is installed on the NGFW Engine.



Add an Access rule to forward traffic

Add Access rules to forward traffic to Web Security Cloud.

Before you begin

- In the cloud Security Portal, you have configured an EasyConnect service.
- In the SMC Management Client, you have created a Proxy Server element that represents Web Security Cloud.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**.
- 2) Browse to **Policies > Firewall Policies**.
- 3) Right-click a policy, then select **Edit Firewall Policy**.
- 4) Add an Access rule that forwards the traffic to Web Security Cloud.
- 5) Click  **Save and Install**.

Example Access rule

Source	Destination	Service	Action
Original source address of the traffic. For example, clients in the internal network.	Original destination address of the traffic. For example, a web server.	The HTTP and TLS Network Application elements.	Allow . Action options: Proxy Server selected for the Forward Traffic to option.

Next steps

To verify that the forwarding works correctly, enable logging and verify from the Logs view that the destination address is translated to the Proxy Server address when this rule matches. For more detailed log data, see the Transaction Viewer in the cloud Security Portal.

Using NAT rules

You can use NAT rules to forward traffic that uses the HTTP and TLS Network Applications to Forcepoint Web Security Cloud.



Note

This method requires Forcepoint NGFW version 6.5 or higher.

Follow these general steps:

- 1) Configure an EasyConnect service in the cloud Security Portal.
- 2) In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.
- 3) Add a NAT rule that selects the traffic to forward. You must define both source and destination NAT.

Related tasks

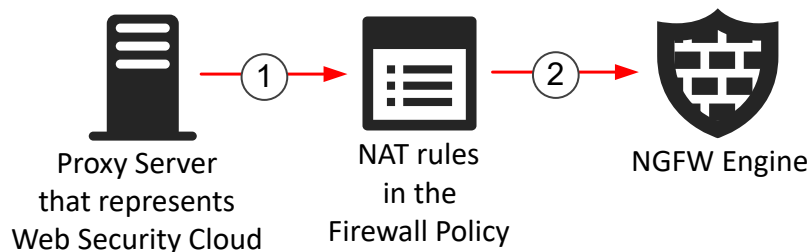
Configure an EasyConnect service in the cloud Security Portal on page 5

Create a Proxy Server element that represents Web Security Cloud on page 6

Add a NAT rule to forward traffic on page 13

Elements used when using NAT rules

The following elements are used when using NAT rules to forward web traffic to Web Security Cloud.



- 1 The Proxy Server element is referenced in the NAT rules in the Firewall Policy.
- 2 The Firewall Policy is installed on the NGFW Engine.

Add a NAT rule to forward traffic


Add a NAT rule to forward traffic to Forcepoint Web Security Cloud.

Before you begin

- In the cloud Security Portal, you have configured an EasyConnect service.
- In the SMC Management Client, you have created a Proxy Server element that represents Web Security Cloud.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Configuration**.
- 2) Browse to **Policies > Firewall Policies**.

- 3) Right-click a policy, then select **Edit Firewall Policy**.
- 4) Add a NAT rule that forwards the traffic to Web Security Cloud.
- 5) Click  **Save and Install**.

Example NAT rule

Source	Destination	Service	NAT
Original source address of the traffic. For example, clients in the internal network.	Original destination address of the traffic. For example, a web server.	The HTTP and TLS Network Application elements.	<p>On the Source translation tab, select Dynamic as the Translation Type, then select the Outbound Multi-Link element that represents your public IP addresses. If you have only one IP address, click Address, then enter the address.</p> <p>On the Destination translation tab, select Forward to Proxy as the Translation Type, then select your Proxy Server element.</p>

Next steps

To verify that the forwarding works correctly, enable logging and verify from the Logs view that the destination address is translated to the Proxy Server address when this rule matches. For more detailed log data, see the Transaction Viewer in the cloud Security Portal.

Using a custom Service element

You can use Access rules that use a custom Service element to forward HTTP and HTTPS traffic to Forcepoint Web Security Cloud.



Note

This method requires Forcepoint NGFW version 6.4 or higher.

NAT is automatically applied to the communication between the client and the destination server, including reply packets.

Follow these general steps:

- 1) Configure an EasyConnect service in the cloud Security Portal.
- 2) In the SMC Management Client, create a Proxy Server element that represents Web Security Cloud.
- 3) Create a custom Service element that references the Proxy Server element.
- 4) Define the Access rule that selects traffic for forwarding to Web Security Cloud.

Related tasks

Configure an EasyConnect service in the cloud Security Portal on page 5

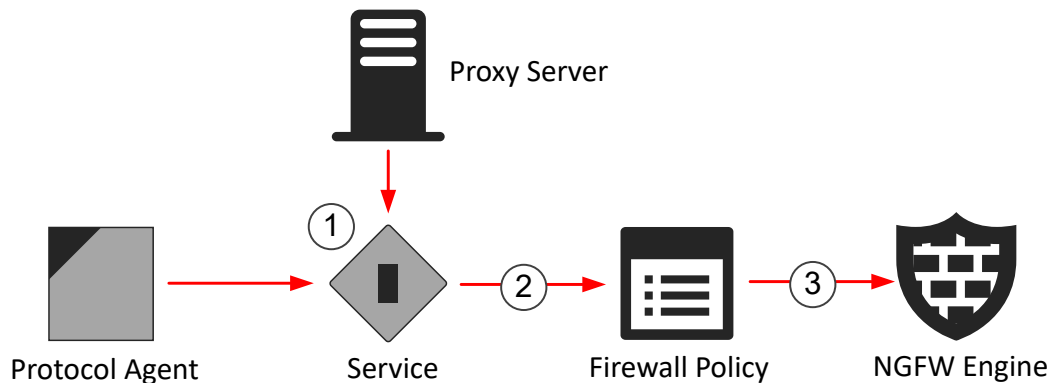
Create a Proxy Server element that represents Web Security Cloud on page 6

Create a custom Service element for forwarding traffic on page 16

Add an Access rule to forward traffic using a custom Service element on page 16

Elements used when using a custom Service element

The following elements are used when using a custom Service element to forward web traffic to Web Security Cloud.



- 1 The Protocol Agent determines the protocol of the traffic that is forwarded. The Service element contains a parameter that defines to which Proxy Server the traffic is forwarded. The Protocol Agent and Proxy Server elements are referenced in the Service element.
- 2 The Service element is referenced in the Firewall Policy.
- 3 The Firewall Policy is installed on the NGFW Engine.


Create a custom Service element for forwarding traffic

In the SMC Management Client, you must create separate custom Service elements for HTTP and HTTPS traffic.

Before you begin

In the SMC Management Client, you have created a Proxy Server element that represents Web Security Cloud.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**.
- 2) Browse to **Other Elements > Services > TCP**.
- 3) Right-click the HTTP or HTTPS service, then select **New > Duplicate**.
- 4) Enter a new name for the Service.
- 5) On the Protocol Parameters tab, select the Proxy Server that represents Web Security Cloud.
- 6) Click **OK**.

Next steps

If you created an element for HTTP, for example, repeat the steps to create the element for HTTPS.

Add an Access rule to forward traffic using a custom Service element


Add Access rules to forward traffic to Web Security Cloud.

Before you begin

- In the cloud Security Portal, you have configured an EasyConnect service.
- In the SMC Management Client, you have created a custom Service element.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**.

- 2) Browse to **Policies > Firewall Policies**.
- 3) Right-click a policy, then select **Edit Firewall Policy**.
- 4) Add an Access rule that forwards the traffic to Web Security Cloud.
- 5) Click  **Save and Install**.

Example Access rule

Source	Destination	Service	Action
Original source address of the traffic. For example, clients in the internal network.	Original destination address of the traffic. For example, a web server.	Custom Service elements that include the Proxy Server that references Web Security Cloud.	Allow

Next steps

To verify that the forwarding works correctly, enable logging and verify from the Logs view that the destination address is translated to the Proxy Server address when this rule matches. For more detailed log data, see the Transaction Viewer in the cloud Security Portal.

Using a policy-based VPN

You can use a policy-based VPN to redirect traffic. Add the Forcepoint NGFW Engine as an Edge Device using the IPsec Advanced feature of Web Security Cloud.



Note

This method requires SMC version 6.1 or higher.

Follow these general steps:

- 1) In the cloud Security Portal, configure Forcepoint Web Security Cloud to receive traffic from the NGFW Engine.
- 2) If SSL decryption is enabled, download the Forcepoint Cloud CA certificate, then add the certificate to client web browsers.
- 3) In the SMC Management Client, import predefined VPN elements for the Web Security Cloud VPN.
- 4) Verify the IKE identity (Phase-1 ID) of the VPN endpoint on the NGFW Engines.
- 5) Edit the Web Security Cloud VPN element that you imported, and add VPN gateways that represent the NGFW Engines.
- 6) Add an Access rule that selects traffic for redirecting to the Web Security Cloud VPN.

Related tasks

Configure Web Security Cloud to receive traffic from Forcepoint NGFW on page 18

Download the Forcepoint Cloud CA certificate on page 19

Import predefined elements for the Web Security Cloud VPN on page 20

Verify the IKE identity (Phase-1 ID) of the VPN endpoint on page 20

Edit the Web Security Cloud VPN on page 21

Add an Access rule to redirect traffic to the Web Security Cloud VPN on page 23


Configure Web Security Cloud to receive traffic from Forcepoint NGFW

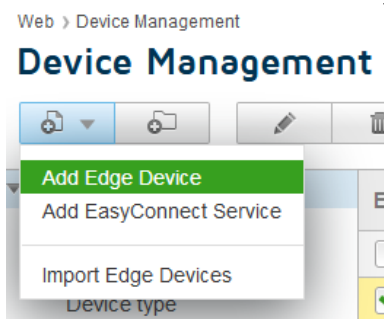
To configure Forcepoint Web Security Cloud to receive traffic from the NGFW Engine, add the NGFW Engine as an Edge Device in the cloud Security Portal.

Steps

1) Log on to the cloud Security Portal at <https://admin.forcepoint.net/portal>.

2) Browse to **Web > Device Management**.

3) Click  **Add > Add Edge Device**.



4) Select **IPsec Advanced** as the **Tunneling Type**.

5) In the **General** section, enter a name and an optional description for the Edge Device.

6) Select **Forcepoint NGFW** from the **Device type** drop-down list.

7) In the **Device Authentication** section, select **IKEv2** from the **IKE version** drop-down list.

8) Select the type of IKE identity (Phase-1 ID) to use from the **IKE identity** drop-down list, then enter the value for the identity.

You can use a DNS name or public IP address as the identity. If you use a DNS name, the value can be a host name or a fully qualified domain name (FQDN). The value does not need to be an existing DNS name or IP address, but it must be the same value that you configure in the SMC Management Client.

- 9) Enter a pre-shared key in the **Pre-shared key** field.
The pre-shared key is the shared secret that must be used when you later configure the VPN in the SMC Management Client.



Tip

To generate a pre-shared key, select **Auto generated new key** from the **Pre-shared key** drop-down list.

- 10) In the **Data Centers** section, select two locations from the list of available data centers.
When you later configure the VPN in the SMC Management Client, you can enable either or both (for high availability) of the data centers in the properties of the Web Security Cloud VPN Gateway. The NGFW Engine does not prioritize one data center over the other.
- 11) In the **Policy Assignment** section, set the default policy for traffic from the NGFW Engine.
- 12) Click **Save**.

Next steps

If your Web Security Cloud Policy enforces SSL decryption, continue by downloading the Forcepoint Cloud CA certificate. Otherwise, continue the configuration by importing the predefined elements for the Web Security Cloud VPN.

Related tasks

Download the Forcepoint Cloud CA certificate on page 19

Import predefined elements for the Web Security Cloud VPN on page 20

Download the Forcepoint Cloud CA certificate

If your Web Security Cloud Policy enforces SSL decryption, you must download and add the Forcepoint Cloud CA certificate as a trusted website signer to client web browsers.

Steps

- 1) Log on to the cloud Security Portal at <https://admin.forcepoint.net/portal>.
- 2) Browse to **Web > Policies**.
- 3) Select the name of your policy.
- 4) On the **Web Categories** tab, click the root certificate link to download the certificate.
- 5) Add the root certificate to client web browsers.


Import predefined elements for the Web Security Cloud VPN

Download and import the predefined elements into the SMC using the SMC Management Client.

Elements in the .zip archive file

Element	Description
Web Security Cloud VPN	A policy-based VPN element for the VPN connection to Web Security Cloud. The VPN has the External VPN Gateway for Web Security Cloud as the central gateway, and uses the Web Security Cloud VPN Profile.
Web Security Cloud VPN Gateway	An External VPN Gateway element for the VPN connection to Web Security Cloud. The External VPN Gateway element includes endpoints that represent different Web Security Cloud data centers.
Web Security Cloud VPN Profile	A VPN Profile element that contains the IKE SA and IPsec SA proposals for the VPN connection to Web Security Cloud.
Web Security Cloud VPN Gateway Profile	A VPN Gateway Profile element that defines the cryptographic suites supported by the VPN Gateway.


Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.


- 1) Go to Knowledge Base article [10582](#), then save the attached .zip archive file in a location that is accessible from the computer where you use the SMC Management Client.
- 2) In the SMC Management Client, select  **Menu** > **File** > **Import** > **Import Elements**.
- 3) Select the .zip archive file, then click **Import**.
- 4) When the import is finished, click **Close**.

Verify the IKE identity (Phase-1 ID) of the VPN endpoint

In the SMC Management Client, open the properties of the NGFW Engine that is used as the local VPN Gateway to connect to Web Security Cloud, then verify that the VPN endpoint uses the same IKE identity (Phase-1 ID) value as configured in the cloud Security Portal.


Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.


- 1) Select  **Configuration**.
- 2) Right-click the NGFW Engine, then select **Edit <element type>**.

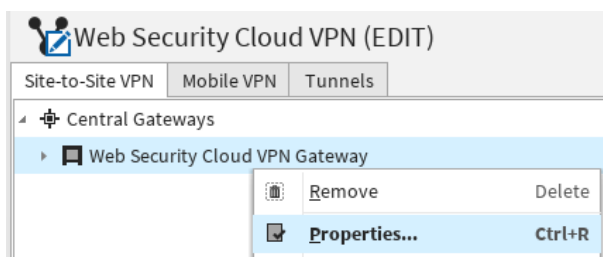
- 3) Browse to **VPN > End-Points**.
- 4) Verify from the **Phase-1 ID** column that the VPN endpoint used to connect to Web Security Cloud uses the same IKE identity (Phase-1 ID) value as configured in the cloud Security Portal.
If necessary, you can use a VPN-specific exception to assign a specific Phase-1 ID value for the Web Security Cloud VPN. Using exceptions allows you to avoid changing the default value that might be used for other VPNs. For more information, see the sections about defining VPN gateways in the *Forcepoint Next Generation Firewall Product Guide*.
- 5) Click  **Save**.

Edit the Web Security Cloud VPN

To enable VPN connectivity between NGFW Engines and Forcepoint Web Security Cloud, use the SMC Management Client to add the VPN gateways that represent your NGFW Engines to the imported Web Security Cloud VPN.

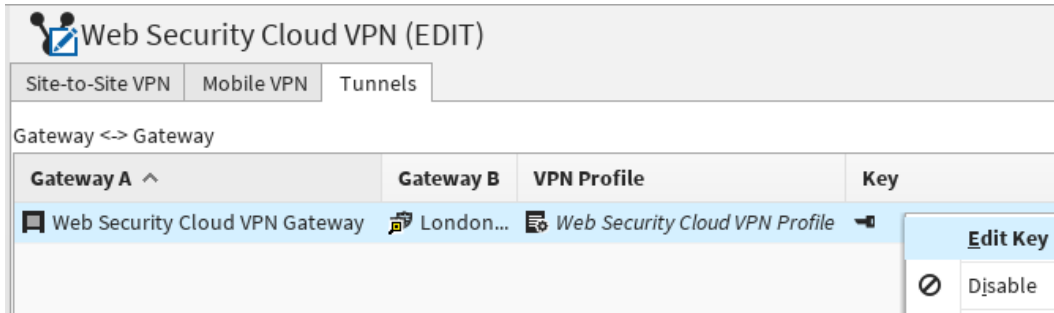
Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**, then browse to **SD-WAN**.
- 2) Browse to **Policy-Based VPNs**.
- 3) Right-click the Web Security Cloud VPN element, then select **Edit**.
- 4) On the **Site-to-Site VPN** tab, right-click the Web Security Cloud VPN Gateway element, then select **Properties**.



- 5) On the **Endpoints** tab, select the external endpoints that correspond to the primary and secondary data centers that you configured in the cloud Security Portal, then click **OK**.
If you do not see the data center that you want to use, see the list of data centers and their IP addresses in Knowledge Base article [16108](#).
- 6) Drag and drop the VPN Gateway element that represents your NGFW Engine from the **Resources** pane to the **Satellite Gateways** pane.

- 7) On the **Tunnels** tab, right-click the **Key** column for the VPN tunnel, then select **Edit Key**.

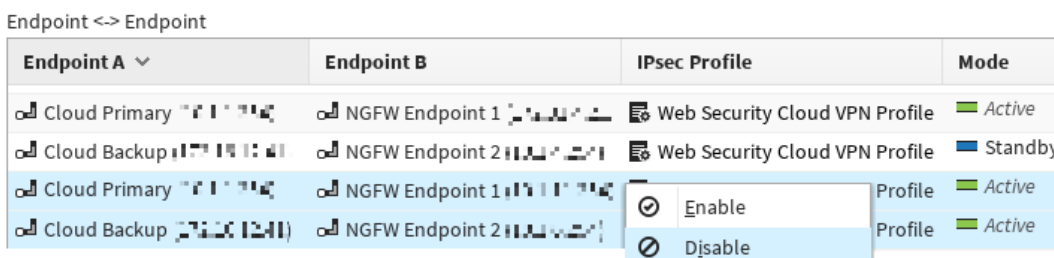


- 8) Replace the pre-shared key with the key that you used in the cloud Security Portal, then click **OK**.
- 9) Right-click the **Mode** column of the tunnel that connects to your secondary data center, then set the mode to **Standby**.

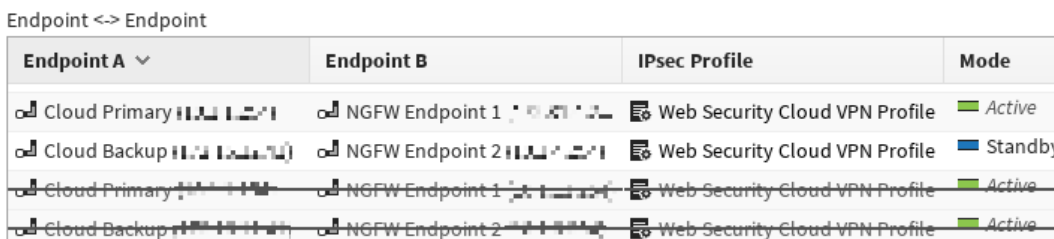


If the primary data center is not available, the secondary data center is automatically used.

- 10) If you have more than one endpoint configured on the NGFW Engine, select all the other tunnels that are available, right-click, then select **Disable**.



- 11) Verify that you have one active tunnel and one standby tunnel only.




- 12) Click **Save**.

Add an Access rule to redirect traffic to the Web Security Cloud VPN

In the SMC Management Client, add an Access rule to redirect traffic to the Forcepoint Web Security Cloud VPN. The Firewall Template policy contains rules that allow the policy-based VPN traffic and maintain the VPN tunnels.

If you use a custom top-level template, you must allow this traffic in the policy. Make sure that at least the ISAKMP (UDP) Service is allowed between the gateways.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**.
- 2) Browse to **Policies > Firewall Policies**.
- 3) Right-click a policy, then select **Edit Firewall Policy**.
- 4) Add an Access rule that redirects the traffic to the Forcepoint Web Security Cloud VPN.

Source	Destination	Service	Action
Local networks	ANY	The HTTP and HTTPS Service elements.	<i>(When the Forcepoint NGFW version is 6.6 or higher)</i> Allow. In the Action options, select Apply VPN as the VPN Action . Select the Web Security Cloud VPN element, then click OK . <i>(When the Forcepoint NGFW version is 6.5 or lower)</i> Use VPN. Select the Web Security Cloud VPN element, then click OK .

- 5) Click  **Save and Install**.

