Introduction

Forcepoint IPsec connectivity is used to securely forward traffic from your network’s edge devices to the cloud service over a virtual private network (VPN). This guide introduces the basics of Forcepoint’s IPsec solution, and provides information on planning and deploying IPsec in your network.

Introduction to the Forcepoint IPsec solution

Internet Protocol Security (IPsec) is an extension to the IP protocol that provides secure traffic tunneling by authenticating and encrypting information sent over a network. Forcepoint IPsec supports transparent end user identification via NTLM, allowing users to browse the Internet without explicitly providing logon credentials.

IPsec uses Authentication Headers (AH) to provide data origin authentication, and Encapsulating Security Payload (ESP) to provide data confidentiality and integrity. Traffic to the Forcepoint IPsec service can be fully encapsulated in tunnel mode, providing complete traffic encryption.

Typical uses for the IPsec service include providing Forcepoint Web Security Cloud protection for:

- Remote offices
- Guest Wi-Fi networks
- Organizations that want to secure traffic sent to the cloud service
- Organizations that have dynamic egress IPs (using IPsec with digital certificate authentication)
- Organizations that do not want a Group Policy Object (GPO) or browser configuration
- Organizations that are unable to or do not want to install an endpoint on client machines
- Organizations with a “bring your own device” policy.
A typical site-to-site IPsec tunneling deployment is shown in the following diagram.

Benefits

Using IPsec to forward traffic to the cloud service can provide a number of benefits. These include:

- There is no need to install endpoint software on client machines or deploy browser configuration PAC files through Group Policy Objects - ideal for BYOD or guest networks.
- Traffic inside the tunnel can be protected via encryption.
- The decryption processing burden is offloaded from end-user devices to the IPsec tunneling infrastructure.
- Your network’s internal IP addresses are available to the cloud service, so:
  - Policies can be created based on internal IP addresses or address ranges.
  - Authentication bypass can be set based on IP addresses or address ranges.
  - Reports can be created using internal IP addresses to identify individual users.
Supported devices

For the latest list of supported devices for use with the Forcepoint IPSec service, see the knowledge base article IPSec configuration settings. Only the devices listed have been tested and verified, but other devices that support Forcepoint’s recommended configuration settings for IPSec, and can forward port 80 and 443 traffic to the tunnel, can be used.

Forcepoint recommends using the latest firmware for your device.

Note

For detailed guidance on configuring Forcepoint NGFW, Cisco, Juniper, and Palo Alto devices for IPSec, please refer to the following articles in the Forcepoint Knowledge Base:

- Forcepoint NGFW
- Cisco
- Juniper
- Palo Alto

You must log in to My Account to access these articles.

Supported standards

Forcepoint Web Security Cloud is compliant with the following drafts of Internet Key Exchange (IKEv1 and IKEv2):

- IKEv1 – RFC 2409/4109 (November 1998/May 2005), supported for PSK and certificate authentication.
- IKEv2 – RFC 5996 (September 2010), supported and recommended for PSK authentication.
Getting started

This chapter outlines the planning and configuration stages required when deploying Forcepoint IPsec connectivity.

Capacity planning

Forcepoint IPsec supports up to 20k connections and 200Mbps per tunnel. To scale beyond this, you will need to split traffic between multiple IPsec tunnels. For example:

- If your requirement is for 10k connections and 500Mbps, you will need 3 tunnels
- If your requirement is for 35k connections and 25Mbps, you will need 2 tunnels.

Redundancy and failover

Forcepoint strongly recommends configuring your device to fail over to another data center cluster to achieve geographic redundancy.

Note

Connection redundancy is a requirement for the Forcepoint Web Security Cloud SLA. Redundancy can be achieved either by using the IPsec service hostname, or by configuring redundant connections to multiple data centers.

For most devices, configure the hostname for the Forcepoint IPsec service as the peer address for your device:

- **vpn.forcepoint.net**
  (Note that this address is .net, not .com.)

This hostname represents multiple geographical data center locations and therefore provide inter-cluster redundancy in the case of a loss of connectivity to one location.
However, you may not be able to use the hostname, or you may wish to connect to specific data center locations. This may be the case if either of the following apply:

- Your device does not support using hostnames as the peer address (for example, Cisco ASA)
- Your organization is governed by data sovereignty regulations that require you to connect to data centers in specific locations.

In these cases, you must configure your device to connect to multiple data center locations, using the appropriate IP addresses.

**Data center locations**

Hostnames and IP addresses for Forcepoint’s IPsec service are listed in the Knowledge Base article [Hostnames and IP addresses for IPsec connectivity](#).

To decide which data centers are best for your environment, consider:

- Which data centers are nearest
- Any geographical or data sovereignty concerns around where users browse or where their reporting data is stored
- The degree of resilience that you want to apply to your deployment.

---

**Note**

Failover behavior, particularly cross-data-center failover, could change an end user’s browsing experience. For example, some sites may change localization or presentation between a UK data center and a German data center (for example, www.google.co.uk might automatically redirect to www.google.de or www.google.nl, depending on which data center users’ traffic is directed through).

Bear in mind that inter-data-center failover should be an exceptional occurrence, so this behaviour might be acceptable in emergency circumstances.

To determine the nearest data center, you can perform a DNS lookup:

```bash
$ nslookup vpn.forcepoint.net
Name:   vpn.gns.forcepoint.net
Address: 86.111.223.181
```

The results of this DNS lookup depend on your DNS configuration, and may not always return the most appropriate data center. Check the returned location against the list in the Knowledge Base article [Hostnames and IP addresses for IPsec connectivity](#). The IP addresses returned may not be the same as those listed in the article.
Device authentication: digital certificate or PSK

Device authentication is required to validate the tunnel at both ends. It verifies that the device connecting to the Forcepoint cloud service belongs to you, and that the service your device is connecting to is a Forcepoint IPsec data center.

Forcepoint IPsec supports two device authentication methods:

- X.509 compliant digital certificates
- Pre-shared key (PSK).

Forcepoint recommends using digital certificates for device authentication, however you can choose which authentication method is right for your organization. The two authentication methods are compared in the following table.

<table>
<thead>
<tr>
<th></th>
<th>Certificate</th>
<th>Pre-shared key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity of setup</td>
<td>More complex: requires knowledge of digital certificate configuration.</td>
<td>Somewhat less complex, and supports bulk management.</td>
</tr>
<tr>
<td>Security</td>
<td>More secure: asymmetric public key cryptography helps to ensure the secrecy of the private key.</td>
<td>Less secure, since PSK relies on all devices having a shared passphrase.</td>
</tr>
<tr>
<td>Scalability</td>
<td>More scalable: can be deployed more easily across multiple devices at different locations.</td>
<td>Less scalable: requires manual configuration of each device with the same shared key.</td>
</tr>
<tr>
<td>Requirements/ recommendations</td>
<td>Does not require a static IP address.</td>
<td>Requires a static external IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The IKEv2 authentication protocol is recommended when using PSK.</td>
</tr>
<tr>
<td>Limitations</td>
<td>Cisco ISR devices require device certificates to be signed by Forcepoint, which adds significant setup overhead. Cisco ASA devices do not support using hostnames as the peering address.</td>
<td>Cannot be used for devices with a dynamic or private external IP address. Cannot be used for devices behind a firewall that performs network address translation (NAT).</td>
</tr>
<tr>
<td>Ideal for</td>
<td>Larger deployments, deployments where the highest levels of secure authentication are required.</td>
<td>For small to medium deployments, or where the organization lacks the expertise to configure digital certificates.</td>
</tr>
</tbody>
</table>
Configuration process

This section details the end-to-end configuration process for setting up your device for IPsec connectivity.

First steps

You will need the following information for each edge device:

- The MAC address of the device
- For certificate authentication: download the Forcepoint intermediate CA.
- For PSK device authentication: the external egress IP address of the device that connects to the cloud service.

If you are a hybrid customer, contact Technical Support to obtain a login to the cloud portal. See Using IPsec with the hybrid service, page 23.

The configuration process is covered step-by-step in Configuration steps, page 10, and is shown as a flow chart in Setup process: flow chart, page 13.

Recommended device configuration settings

See the Knowledge Base article IPsec configuration settings for details of the device configuration settings that are supported for use with the Forcepoint IPsec service. The article details our recommended settings, as well as a number of other configuration options that are also supported.

A configuration checklist is provided for your reference in Configuration checklist, page 14.
This section details the IPsec configuration process. See also:

- Setup process: flow chart
- Configuration checklist

The basic steps to configure IPsec tunneling to the cloud service are as follows.

1. Define the device in the cloud portal.
   
   - Add your edge device via the Web > Device Management page, defining the device name, type, MAC address and an optional description. This requires that your administrator account has the Manage Edge Devices permission enabled. Note: by default, you can create 2 tunnel connections for your account. To add more connections, contact your sales account manager to discuss your requirements.

   See the Forcepoint Web Security Cloud Help - Managing Network Devices for instructions on adding devices.

2. Define whether the device will use PSK or digital certificate authentication.
   
   - For PSK authentication:
     
     a. Enter the egress IP of the edge device. This is the external IP address of the device, from which the cloud service will receive traffic.

     b. Enter or auto-generate a pre-shared key. This key must be used in your device’s connection profile.

     c. Copy the Device ID for your edge device, which appears beneath the Pre-shared key section. This ID includes the device’s MAC address, and is used to identify traffic from the device to the service. You must enter this ID as the device ID (or key ID) in your edge device's connection profile.

     For pure cloud customers, the device ID is in the form: psk.hosted.00~01~02~a3~b4~c5@websense.com
For hybrid customers, the device ID is in the form:

```
psk.hybrid.00-01-02-a3-b4-c5@websense.com
```

### Important

Ensure you enter the device ID exactly as given. Because this ID is used to identify traffic from the device to the cloud service, an invalid device ID can result in the service failing to recognize traffic from the tunnel. In particular, do not use the device’s IP address as the device ID. This may result in the tunnel establishing successfully, but traffic failing to be recognized.

**Note:** Palo Alto devices do not accept the tilde (~) character. For Palo Alto devices, enter the key id as colon-delimited hexadecimal. See the [Palo Alto](#) article in the Forcepoint Knowledge Base for more information.

#### For digital certificate authentication:

a. Import a valid certificate authority (CA) file to the Security Portal, encoded in PEM format. (Your edge device may be able to generate a CA, or you can use a tool such as OpenSSL.) This CA is used to authenticate your device’s identity certificate.

b. Create an identity certificate that your device will present to the cloud service for authentication. (You may be able to create this on your device, or you can generate a certificate within the cloud portal and download it.) The certificate must include the device’s MAC address as the “Common Name”.

   If using a Cisco ISR device, you must create a certificate signing request on your device, and send it to Forcepoint Technical Support for the certificate to be signed with the Forcepoint certificate authority.

   For further information on generating an identity certificate for your device, see [Generating device certificates, page 19](#).

c. Import the Forcepoint public intermediate CA to your edge device. This is used to verify that you are connecting to the Forcepoint IPsec service.

3. Create a connection profile for your tunnel.

   For Forcepoint NGFW devices, download and import the NGFW setup ZIP file, which you can download from the Knowledge Base article [Configure Forcepoint NGFW to redirect web traffic to Web Security Cloud](#). This file includes predefined elements which can be imported to create your tunnel. The article includes instructions on how to import this to your NGFW device. Once this is completed, skip to step 6.
For all other devices, create a connection profile to connect to the appropriate Forcepoint IPsec peer hostnames/IP addresses. (See the article Hostnames and IP addresses for IPsec connectivity.)

4. Define IKE authentication settings on your edge device. For instructions on how to do this on specific devices, see the following articles in the Forcepoint Knowledge Base:
   - Forcepoint NGFW
   - Cisco
   - Juniper
   - Palo Alto

You must log in to My Account to access these articles.

5. If you used an IP address as the peer address for your tunnel (such as on a Cisco ASA or Palo Alto device), you must manually configure a second tunnel to a different data center for redundancy. This is required for the Forcepoint Web Security Cloud SLA. Repeat steps 3 and 4.

6. If required, configure NAT exemptions to ensure that network address translation is not applied to traffic from client networks that is to be routed through the tunnel. (See How do I configure my Cisco device to connect to Forcepoint IPsec?)

7. Browse to the proxy query URL to make sure that the appropriate policy is being applied to your tunnel. (Also see Test your policies, page 18.)

The query URL is:
http://query.webdefence.global.blackspider.com/?with=all

**Maximum segment size (MSS)**

The encapsulation overhead of the IPsec tunnel means that TCP sessions sent over the tunnel must be limited to a lower Maximum Segment Size (MSS) than usual. Most TCP clients will propose an MSS value of 1460 bytes when connecting over an Ethernet network.

Forcepoint recommends setting an MSS value of no more than 1360 bytes in order to leave overhead for IPsec encapsulation. This can often be achieved by using the MSS clamping feature of a firewall or router, to ensure that any TCP traffic sent down the tunnel is limited to an MSS value of 1360.

Where the WAN connection to Forcepoint’s data centers is using the IPoE or PPPoE protocol, the MSS value may need to be lower still, to account for the encapsulation overhead of the WAN connection.

To display the current MSS setting for your tunnel interface, use the appropriate “show interface” command on your edge device.
Setup process: flow chart

**PLANNING**
Ensure your planning has taken into account:
- Required tunnel capacity
- Failover strategy
- Preferred authentication method
- Any device-specific limitations
Gather the following information/resources:
- Device MAC addresses
- Forcepoint root CA (for certificate authentication)
- External IP addresses (for PSK authentication)

**BEFORE YOU BEGIN**
Request login credentials for the Forcepoint Security Portal from Technical Support.
Use the Security Portal Help to guide you through adding your devices.

**PORTAL CONFIGURATION**

1. Log on to the Security Portal.
2. Add your devices via Web > Device Management.
3a. Generate a device certificate authority (using your device or OpenSSL), and upload it to the portal.
4. Are you using PSK or certificate authentication?
5. In the cloud portal:
   - Add the device egress IP
   - Create or generate an encryption key
   - Copy the device ID

**DEVICE CONFIGURATION**

6. Are you using a Cisco ISR device?
7a. Create an identity certificate for your device (on the device itself, or within the cloud portal).
7b. Create a certificate signing request (CSR) on your device and send it to Forcepoint Technical Support to be signed.
7c. Upload the signed certificate to your device.
8. Import the Forcepoint public root certificate authority to your device.
9. On your device:
   - Create a connection profile
   - Define IKE authentication settings for tunnel establishment
   - Configure NAT exemptions (if required)
10. Are you using a Stonesoft device?
11. Are you using the hostname or an IP address as the peer address for your tunnel?
12. Create a second tunnel, using a different data center IP address (repeat step 10).

**TESTING**
Verify that your traffic is being filtered using the proxy query page.

**SETUP COMPLETE**
## Configuration checklist

### Edge device configuration checklist

<table>
<thead>
<tr>
<th>Platform</th>
<th>☐ Forcepoint NGFW</th>
<th>☐ Juniper SRX</th>
<th>☐ Cisco ISR</th>
<th>☐ Juniper SSG</th>
<th>☐ Cisco ASA</th>
<th>☐ Palo Alto</th>
</tr>
</thead>
</table>

### Encryption details

<table>
<thead>
<tr>
<th>Device authentication type</th>
<th>Phase 1 (IKE)</th>
<th>Phase 2 (ESP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKEv1:</td>
<td>PSK (Main Mode only)</td>
<td>SHA-1 (recommended)</td>
</tr>
<tr>
<td></td>
<td>Certificate</td>
<td>SHA-1 (recommended)</td>
</tr>
<tr>
<td></td>
<td>Or IKEv2: (recommended for PSK)</td>
<td>SHA-256 (with AES encryption only)</td>
</tr>
<tr>
<td></td>
<td>PSK (Main Mode only)</td>
<td>SHA-256 (with AES encryption only)</td>
</tr>
</tbody>
</table>

| Authentication              | ☐ SHA-1 (recommended)                             | ☐ SHA-1 (recommended)                             |
|                            | ☐ SHA-256 (with AES encryption only)              | ☐ SHA-256 (with AES encryption only)              |

| Encryption                 | ☐ AES-128                                         | ☐ NULL                                           |
|                            | ☐ 3DES                                            | ☐ AES-128                                        |

| DH Group                   | ☐ Group 5 (recommended)                           | ☐ PFS disabled                                   |
|                            | ☐ Group 2                                         |                                                  |
|                            | ☐ Group 14                                        |                                                  |

| Lifetime                   | 86400s                                           | 28800s                                           |

### Network information

| MAC address:               | e.g. 11:22:33:44:55:66                           |
|                           |                                                  |
| External egress IP:       | PSK only                                         |
|                           |                                                  |
| Downloaded the Forcepoint public CA | ☐ Yes                                           |
|                           | Certificate only                                 |
| Forcepoint host configured| ☐ vpn.forcepoint.net (recommended)               |
|                           | ☐ IP address                                     |
|                           | Cisco ASA and Palo Alto devices must use IP addresses. |
| Backup tunnel configured? | ☐ Yes                                            |
|                           | Required if an IP address is used as the peer address |
| NAT-T                     | ☐ Enabled                                        |
| NAT Keep-alive            | ☐ Enabled, interval of 10s                       |
| DPD                       | ☐ Enabled, 10s timeout                            |
| ESP tunnel #1 subnet      | e.g. 10.12.1.0/24                                |
|                           |                                                  |
| ESP tunnel #2 subnet      |                                                  |
|                           |                                                  |
| ESP tunnel #3 subnet      |                                                  |
|                           |                                                  |
| ESP tunnel #4 subnet      |                                                  |
|                           |                                                  |
| ESP tunnel #5 subnet      |                                                  |
|                           |                                                  |
| ESP tunnel #6 subnet      |                                                  |
|                           |                                                  |
Once you have completed the setup steps in the preceding section, your next steps are to:

- Enable notification pages for HTTPS sites (if required)
- Set up end-user authentication (if required)
- Configure browsers for NTLM identification (if required)
- Ensure you have configured policies to manage traffic from your network. See Forcepoint Web Security Cloud Help - Defining Web Policies for information on policy configuration.
- Test your policies.

**Enable notification pages for HTTPS sites**

In order for notification pages to be displayed for HTTPS sites - for example, block pages if the website is in a category that is blocked, or the Pre-logon welcome page for authentication - you must configure a root certificate on each client machine. This acts as a Certificate Authority for secure requests to the cloud proxy.

The setting is found on the Web > Block & Notification Pages page, under Settings. To enable it, mark the checkbox Use certificate to serve notifications for HTTPS pages.

This page also has a link to download the Forcepoint root certificate, which should be installed on client machines. For further details, see Forcepoint Web Security Cloud Help - Configure Block & Notification Pages.

**Set up end-user authentication**

End-user authentication is driven by the setting configured in your Web policy. For IPsec traffic, the cloud service can perform either NTLM identification or manual authentication. NTLM identification uses the credentials presented by a user’s browser, and compares these to the user details you have synchronized with the cloud...
service in order to identify the user. Manual authentication requires users to log on before they can browse, using the email address and password registered with the cloud service.

The following graphic shows the **Access Control** tab in the Forcepoint Security Portal, used to define your authentication settings.

![Access Control Tab](image)

By default, manual authentication is enabled. If the **Always authenticate users on first access** option is set, users are prompted to authenticate when first logging on.

If NTLM identification is enabled, it is given priority and will be used instead of manual authentication. In order for NTLM identification to work seamlessly, you must synchronize end user information including NTLM IDs with the cloud service. (See [Forcepoint Security Portal Help - Directory Synchronization](#)). If a user cannot be identified via NTLM, the service defaults to manual authentication.

For further information on setting up end-user authentication, see [Forcepoint Web Security Cloud Help - Access Control tab](#).

---

**Note**

Currently, single sign-on, the endpoint client, and secure form-based authentication are not supported for use with Forcepoint IPsec. See [Limitations, page 27](#).
Authentication bypass

Both cloud and hybrid administrators can elect to bypass authentication based on internal IP addresses, ranges, or subnets. Forcepoint Technical Support must enable the Internal Bypass Rules for Edge Devices feature for your account. See Forcepoint Web Security Cloud Help - Bypassing authentication settings for more information.

Configure browsers for NTLM identification

NTLM identification also requires that you add the authentication URLs for the Forcepoint cloud service to your browsers’ local intranet zone.

The following URLs must be trusted:

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

For guidance on adding these URLs for various browsers, see the following article in the Forcepoint Knowledge Base: Configuring browsers for NTLM identification.
Test your policies

Your policies can be tested using the proxy query page:

http://query.webdefence.global.blackspider.com/?with=all

Verify that traffic is going through the cloud service and that the correct policies are being applied. The following graphic shows the result of a successful test.

Confirmation Page

Yes, you are using the Filtering Proxy Server

Server Information

Version 7.9.50787.265
Hostname pc32g.srv.mailcontrol.com

Policy chain

Customer name Policy name
Shows your account and policy information

Connection information

Your external IP address
Proxy 1.1 hosted websense 32g

HTTP headers

via 1.1 hosted websense 32g
accept-language en-US,en,q=0.5
accept-encoding gzip, deflate
x-forwarded-for 204.15.64.187
accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
user-agent Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
host query.webdefence.global.blackspider.com
client-ip unspecified
Generating device certificates

A device certificate is presented by your edge device to the cloud service to authenticate the fact that the connecting device belongs to you. There are three options for generating a certificate for your device:

- Generate the certificate on your device
- Generate the certificate in the cloud portal (see Using the portal to generate a certificate, page 19. (Contact Forcepoint Technical Support if you do not have access to this feature.)
- Use a third-party tool such as OpenSSL. See Using OpenSSL to generate a certificate, page 20.

If you are using the hybrid service and do not have a portal account, a Forcepoint Technical Support representative can import the certificate to the cloud service on your behalf.

Using the portal to generate a certificate

A feature is available that allows administrators to generate the device certificate from within the cloud portal. This can either be done while adding the edge device in the portal, or later, after the device has been added. To enable this feature, Forcepoint Technical Support must enable the Device Certificate Generation feature for an account.

For further information, see Forcepoint Web Security Cloud Help - Generating device certificates.

To generate a device certificate in the cloud portal, you must have access to the CA’s private key file and its associated passphrase. The private key file has a name such as “cakey.pem.” It is either provided with a purchased CA or generated with a self-signed CA.
For security reasons, the private key data is not saved after the certificate is generated. This means you must enter the key and passphrase each time you generate a device certificate for this certificate authority.

---

**Note**

Customers using Cisco ISR cannot generate device certificates within the portal. With ISR, the certificate signing request (CSR) must be generated on the device and sent to Forcepoint Technical Support to be signed using Forcepoint’s certificate authority.

See the Knowledge Base article How do I configure my Cisco device to connect to Forcepoint IPsec?

---

**Using OpenSSL to generate a certificate**

This section does not provide a comprehensive tutorial on how to use OpenSSL. It lists a few points that are relevant to generating your own certificates and CAs. It assumes that you are familiar with OpenSSL and have a working OpenSSL installation.

**Generating a CA**

The following steps are used to generate a CA using OpenSSL. Ensure you have root permissions on your Linux machine before beginning this process.

1. Create the following directory:
   - `/root/ca` – to store the openssl.cnf file and run openssl commands

2. Within the `/root/ca` directory, create the following sub-directories:
   - `ca` – to store the CA certificate
   - `certs` – to store the user/identity certificates
   - `csr` – for certificate signing request
   - `private` – to store the private key for the CA certificate

3. Copy the file openssl.cnf to the `/root/ca` directory.
   By default, OpenSSL uses the configuration file `openssl.cnf` for certificate generation. This configuration file should be available as part of the OpenSSL installation. A copy of this configuration file can be made and modified to suit the needs of the organization that generates the certificate.

4. Run the following commands from the `/root/ca` directory:
   ```
   touch index.txt
   echo 1000 > serial
   ```

5. Run the following command from the /root/ca directory to create the Certificate Authority and private key.
Generating device certificates

```bash
openssl req -new -x509 -days 3650 -extensions v3_ca -keyout private/ca.key.pem -out ca/ca.cert.pem
```

This command creates a 2048-bit RSA private key and a self-signed CA certificate with a validity period of 10 years (3650 days). Fill in the certificate authority information as accurately as possible, remembering to enter the private key.

The following command can be used to list the properties of a CA certificate, and to verify whether the details supplied during the CA creation process have been inserted correctly:

```bash
openssl x509 -in ca/cacert.pem -text
```

Generating an identity certificate signing request

Use the following steps to create a certificate signing request.

1. Run the following command from the `/root/ca` directory:

   ```bash
   openssl req -new -nodes -keyout certs/client.key -out csr/client.csr -days 365
   ```

   This command creates a 2048-bit strong RSA private key and a certificate signing request signed by the CA. 365 is the number of days until the certificate expires. It is not necessary that the strength of the key be 2048 bits. You may choose to use a different strength for compliance reasons. Generating an identity certificate using the above command involves providing several parameters.

   The important parameter to specify is **Common Name**. This field should contain the MAC address of the device that is being configured. This MAC address is provisioned in your cloud account. It is also necessary to specify the keyword **Hybrid** if you intend to use the hybrid service.

   For example, if the MAC address of the device is “00:0C:29:D7:74:8E” and you are using the hybrid service, the certificate should bear the subject **Hybrid 00:0C:29:D7:74:8E**.

   If you are using the cloud service, the certificate must consist only of the MAC address of the device.

2. Once you have generated the CSR, copy and paste it into a text file. Save the file as a `.csr` file (for example, ipsec.csr). Save the file to the `/root/ca/csr` directory

---

**Important**

Each device must use its own certificate for IPsec connectivity. Using the same identity certificate in more than one device results in an unstable deployment.
Generating device certificates

Signing the certificate with CA

Once the identity certificate is created, it can be signed using the CA that was generated earlier.

---

**Note**

Customers using Cisco ISR devices cannot sign their own certificates. The certificate signing request (CSR) must be generated on the device and sent to [Forcepoint Technical Support](#) to be signed using Forcepoint’s certificate authority.

---

To sign the identity certificate using your CA:

1. Run the following OpenSSL command from the `/root/ca` directory:

   ```bash
   openssl ca -config openssl.cnf -policy policy_anything -out certs/client.crt -infiles csr/ipsec.csr
   ```

   This command signs the identity certificate signing request created in the previous section. To sign the certificate signing request, the key to the CA is required.

---

**Note**

The above command uses the configuration file `openssl.cnf`. The default configuration file shipped in most OpenSSL packages can be used, or you can change the default parameters in the configuration file to suit your specific needs.

---

At this point, you should have the following files:

- `ca.key.pem` (private key)
- `ca.cert.pem` (certificate authority cert)
- `ipsec.csr` (certificate signing request)
- `IPsecSignedCert.crt` (signed certificate)

2. Use a program such as WinSCP to copy the files from your Linux machine.
Using IPsec with the hybrid service

If you are using Forcepoint Web Security Cloud with the hybrid service, the following additional steps are required:

- If you do not have a cloud portal account, contact Forcepoint Technical Support to add your edge device details in the cloud before setting up your device.
- Special Sync Service configuration is required. See IP-based policy enforcement in hybrid deployments, page 23.
- If you have installed the Forcepoint root certificate and wish to see notification pages, in the Forcepoint Security Manager, navigate to Web > Settings > Hybrid Configuration > User Access > HTTPS Notification Pages, and mark the Use the hybrid SSL certificate... checkbox. This ensures that notification pages (such as block pages) are displayed for HTTPS requests.

---

IP-based policy enforcement in hybrid deployments

In order to use IP address-based policies for users whose requests go through the hybrid service, a configuration change is required on the Sync Service machine.

1. Log on to the Sync Service machine with Administrator privileges.
2. Navigate to the Websense\bin directory:
   - Linux:
     /opt/Websense/bin
   - Windows:
     c:\Program Files\Websense\Web Security\bin
or

c:\Program Files (x86)\Websense\Web Security\bin

3. Open the **SyncService.ini** file in a text editor.
4. Add the following line under the “SyncServiceHTTPPort” entry:
   
   ```
   OptimizePolicyExtract=False
   ```
   
   When you are finished, the file will look something like this:
   ```
   [service]
   SyncServiceHTTPAddress = <ip_address>
   SyncServiceHTTPPort = 55832
   OptimizePolicyExtract=False
   ```

5. Save and close the file.

6. Use the Windows Services tool or the /opt/Websense/WebsenseDaemonControl command to restart Sync Service.
Forcepoint makes the following recommendations as best practices when configuring your IPsec solution.

- **Device authentication:**
  - Forcepoint recommends using digital certificates over PSK. Digital certificates are the most secure and scalable authentication option, though using certificates increases the complexity of setup, which some organizations may find prohibitive.
  - If using PSK for device authentication, using the IKEv2 authentication protocol for tunnel negotiation is recommended.

- **Encryption algorithms for IKE negotiation:**
  - For IKEv1 phase 1 negotiation, Forcepoint recommends AES-128 encryption. DES/3DES encryption are also supported for this phase.
  - For IKEv1 phase 2 negotiation, Forcepoint recommends NULL encryption for best performance. AES-128 is also supported for this phase, but may result in decreased throughput.

- **Traffic routing:** Forcepoint IPsec supports web traffic only (HTTP and HTTPS). Other traffic, such as SMTP and FTP, must be routed outside of the tunnel, directly to the relevant destination.

- **NAT traversal:** NAT-T must be enabled on your edge device.

- **On some devices, when using PSK authentication, an additional peer ID parameter must be set. This parameter is required for Cisco ISR (parameter name: “remote-identity”), and Juniper SRX (parameter name: “match identity user-fqdn”).**
  
  The peer ID parameter must be set to **vpn-proxy.websense.net**. (Note: this parameter is separate to the service hostname, vpn.forcepoint.net. The parameter provides a unique identifier string to the cloud service, and is not a resolvable hostname.)

  For further information on configuring this parameter on Cisco ISR and Juniper SRX devices, see the [Cisco](#) and [Juniper](#) configuration articles in the Forcepoint Knowledge Base.

  Note that if you are using a device that is not on Forcepoint’s supported device list, this parameter may also be required.
Google QUIC protocol: as a best practice, Forcepoint recommends adding a firewall rule to block UDP on port 443. This prevents Google Chrome browsers from accessing Google services directly via the experimental QUIC protocol. For further information, see the knowledge base article [Google QUIC protocol is not supported by the Forcepoint cloud service](#).
The following items are known limitations of the Forcepoint IPsec solution.

- To support PAC file enforcement, you must use the alternate (port 80/443) PAC file address. The standard PAC file address (using port 8082/8087) is not supported.
- Forcepoint Web Security Endpoint is not supported for use with Forcepoint IPsec.
- Certificate authentication is not supported with IKEv2.
- The service does not support certificate revocation lists for invalid certificates.
- The service does not support self-signed identity certificates.
- Secure form-based authentication is not supported for use with Forcepoint IPsec.
- Using an authentication bypass rule to force NTLM, basic authentication, or the welcome page does not work with IPsec tunneling if a URL destination is configured.
- Basic authentication does not work for iTunes with IPsec tunneling.
- Single sign-on using the SAML standard is not supported for use with Forcepoint IPsec.
- Windows XP support: SSL decryption and scanning of HTTPS traffic for Internet Explorer on Windows XP is not possible, since it does not support Server Name Indication (SNI). SNI is required for HTTPS decryption, to extract the destination hostname and create a decryption certificate.
- Dropbox is not supported for use with the Protected Cloud Apps feature in Forcepoint Web Security Cloud with IPsec tunneling.
- Forcepoint’s virtual point of presence (vPoP) IP addresses cannot be used with IPsec tunneling.
- Some web pages may not load properly in Safari after successful user authentication. Ensure the Block cookies option is set to Never in Safari’s privacy preferences.
End-user client requirements

Forcepoint IPsec has the following requirements for Internet Explorer and Safari:

- Internet Explorer: version 7 and above is required. Versions earlier than this do not support SNI, which is required by Forcepoint IPsec.
- Safari: if the customer policy has authentication enabled, Safari users must change the **Block cookies** setting to **Never** to ensure web pages load properly:
The following table lists some problems that may be encountered in configuring and establishing your tunnel, with some suggested actions.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Suggested actions</th>
</tr>
</thead>
</table>
| Your tunnel cannot be established            | Check the settings for your tunnel against the recommended settings detailed in the article IPsec configuration settings. Run through the Configuration checklist, page 14.  
  Check that the following items were correctly entered in your device’s connection profile:  
  ● Connection hostname or IP address  
  ● Device ID  
  If an invalid Device ID is configured on the device, the tunnel may fail to establish, or traffic from the device may not be recognized. The device ID must be in the format:  
  psk.<service>,<tilde separated mac address>@websense.com  
  For example:  
  psk.hosted.ff–ff–ff–ff–ff@websense.com  
  psk.hybrid.ff–ff–ff–ff–ff@websense.com  
  Note: using the device’s IP address as the device ID can result in successful tunnel establishment, but users will see authentication prompts when browsing, because the service fails to match traffic to the device. |
| Your device has previously connected, but cannot re-establish the tunnel | Check the settings for your tunnel against the recommended settings detailed in the article IPsec configuration settings. Run through the Configuration checklist, page 14.  
  In particular, check you are using supported DH group settings. When incorrectly set, these settings can cause problems at the renegotiation stage.  
  Clear the IPSec security associations on your device, and attempt to re-establish the tunnel.  
  Tip: while testing, temporarily set the Lifetime value for your connection to a low value (such as 10 minutes) to check whether the tunnel can successfully re-establish. Once the tunnel is re-establishing correctly, revert the lifetime to the recommended value. |
### Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Suggested actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your tunnel has successfully established, but your policy settings are not being applied</td>
<td>Use the proxy query page to identify which policy is being applied. If necessary, revisit your policy settings. See <em>Test your policies, page 18.</em></td>
</tr>
<tr>
<td>The policy test page is showing the correct policy, but some HTTPS connections are being closed. (HTTP requests are working.)</td>
<td>Ensure you have checked the <strong>Use certificate to serve notifications for HTTPS pages</strong> in the cloud portal, on the <strong>Web &gt; Block &amp; Notification Pages</strong> page, under Settings. See <em>Enable notification pages for HTTPS sites, page 15.</em></td>
</tr>
</tbody>
</table>
| End users see authentication popups when browsing; NTLM identification is not working | Use the proxy query page to identify which policy is being applied. If necessary, revisit your policy settings. See *Test your policies, page 18.*  
Check your NTLM settings. See *Set up end-user authentication, page 15* and *Configure browsers for NTLM identification, page 17.*  
Ensure that your directory synchronization has successfully imported users and groups.  
Ensure you have entered the edge device’s device ID (or key ID) exactly as given in the cloud portal. Using the device’s IP address can result in successful tunnel establishment, but users will see authentication prompts when browsing, because the service fails to match traffic to the device. |
| Block pages are not displaying for HTTPS sites                         | Ensure you have checked the **Use certificate to serve notifications for HTTPS pages** in the cloud portal, on the **Web > Block & Notification Pages** page, under Settings. See *Enable notification pages for HTTPS sites, page 15.* |

If you continue to have issues after checking all the items above, please contact Technical Support. To aid troubleshooting, please complete the *Configuration checklist* and provide this information to your support representative.

## Troubleshooting with HAR files

To help diagnose network issues, you can generate a .HAR (HTTP Archive) file to log your browser’s interaction with a particular website. HAR files can be generated using Google Chrome’s Developer Tools, as well as other software packages.
Troubleshooting your third-party device

For specific troubleshooting advice on Cisco, Juniper, and Palo Alto devices, see the following Knowledge Base articles. These articles include device-specific tips and commands you can use to troubleshoot your connection:

- [Cisco](#)
- [Juniper](#)
- [Palo Alto](#)