Forcepoint

Web Security Cloud

IPsec Advanced Configuration Guide

Revision A

Contents

Introduction

IPsec Advanced is Forcepoint's next generation IPsec service, based on Forcepoint's NGFW technology. IPsec Advanced is used to forward traffic securely from your network's edge devices to the cloud service over a virtual private network (VPN). This guide covers the Forcepoint Advanced IPsec solution, introduced in July 2019, and provides information on planning and deploying IPsec for your network.

Important

This guide covers the Forcepoint Advanced IPsec solution, launched in July 2019. IPsec Advanced is the platform for which future features will be developed, and supports wide device interoperability, and devices with dynamic IP addresses using pre-shared key authentication.

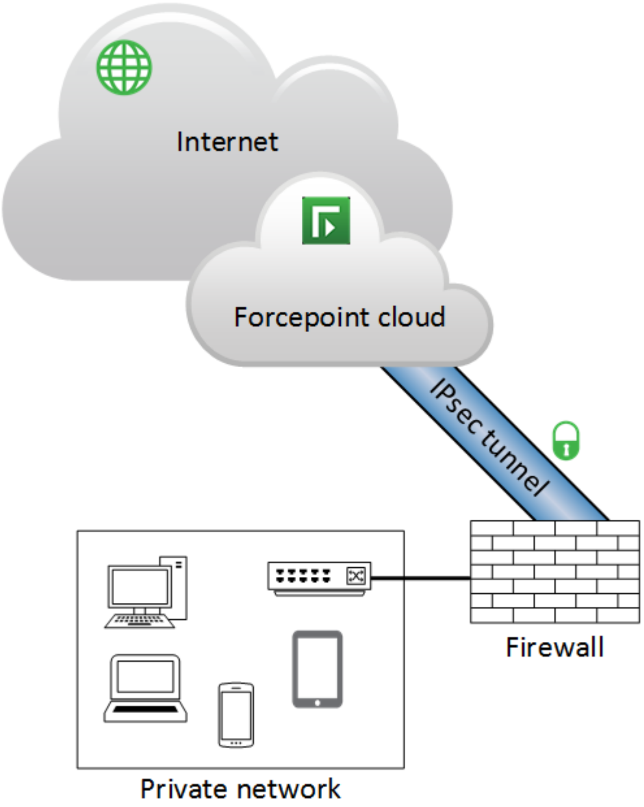
Introduction to Forcepoint IPsec Advanced

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. The IPsec protocol uses Internet Key Exchange (IKE) to establish session keys for encryption and decryption, and Encapsulating Security Payload (ESP) to provide data confidentiality and integrity. Traffic to the Forcepoint IPsec Advanced service can be fully encapsulated in tunnel mode, providing complete traffic encryption.

Forcepoint IPsec Advanced supports transparent end user identification via NTLM, allowing users to browse the Internet without explicitly providing logon credentials. Typical uses for the IPsec Advanced 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
- 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 Advanced 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
- Your network’s internal IP addresses are available to the cloud service, so:
  - Policies can be created based on internal IP addresses, address ranges, or subnets
  - Authentication bypass can be set based on IP addresses, address ranges, or subnets
  - Reports can be created using internal IP addresses to identify individual users.

Capacity planning

Forcepoint IPsec Advanced supports up to 5Gbps throughput per tunnel and 1,000,000 concurrent connections.

By default, tunnels are configured for 200Mbps throughput. Customers requiring more than the default can submit a request to Forcepoint Technical Support.

Supported devices

Forcepoint IPsec Advanced is a standards-based service. Any edge device that supports our recommended configuration settings, and can forward port 80 and 443 traffic to the tunnel, can be used to forward traffic to the service. See *Recommended settings and best practices*.

For the latest list of devices that have been tested and accredited for use with the Forcepoint IPsec Advanced service, see the knowledge base article IPsec Advanced supported devices.

Forcepoint recommends using the latest firmware for your device.

Use the **Cloud Service Status** option provided in the banner of the Cloud Security Gateway Portal for tunnel system status. You must first subscribe to the physical data center connected to the Points of Presence configured on the **Web** > **Device Management** page of the portal.

Configuration guides

See the following articles in the Forcepoint Knowledge Base for detailed configuration guidance for the following devices:

- Cisco ASA/FTD
- Cisco ISR
- Juniper SRX
- Juniper SSG

Related concepts
Recommended settings and best practices on page 11

Supported standards

Forcepoint Web Security Cloud is compliant with the following drafts of Internet Key Exchange:

- IKEv1 – RFC 2409/4109 (November 1998/May 2005)
- IKEv2 – RFC 7296 (October 2014)

Configuration process

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

First steps

You will need either the public IP address, or DNS hostname of the device, to use as the IKE ID:

- Use the public (egress) IP address of the edge device as the IKE ID if the public IP address is static.
- Use the DNS hostname (FQDN) of the device, with IKEv2, if your device has a dynamic IP address.

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

The configuration process is covered step-by-step in *Tunnel configuration*.

See *Recommended settings and best practices*, for details of the recommended and supported device configuration settings for IPsec Advanced. The section also details device configuration best practices.

Related concepts
Using IPsec with the hybrid service on page 10
Recommended settings and best practices on page 11

Related tasks
Tunnel configuration on page 5

Tunnel configuration

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

1) Define the device in the cloud portal via the **Web** > **Device Management** page. See the Forcepoint Web Security Cloud Help - Managing Network Devices for instructions on adding devices.

> **Note**
>
> By default, you can create 200 tunnel connections for your account. To add more connections, contact your sales account manager to discuss your requirements.

2) On your device, create a connection profile for your tunnel, using the supported settings documented in *Recommended settings and best practices*.
The following generic steps are required for any supported device:

   a) Create an IKE proposal (IKEv2 is recommended).

   b) Create an IPsec proposal (AES-GCM algorithm is recommended).

   c) For authentication, configure the pre-shared key configured in the cloud portal.

   d) For the IKE ID, use the egress IP address, or DNS hostname of the device, as selected in the cloud portal.

   e) Add a policy or filters to route port 80 and 443 traffic to the tunnel.

   f) Set up an IKE gateway, specifying the Forcepoint point of presence (data center or local PoP) IP address, as selected in the cloud portal. IP addresses for IPsec Advanced are listed in the article IP addresses for GRE and IPsec Advanced connectivity.

   g) Ensure you configure your device for geographic redundancy, using both the primary and secondary tunnel addresses. See *Redundancy and failover*.

3) 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.

4) Browse to the proxy query URL to make sure that the appropriate policy is being applied to your tunnel. (Also see *Test your policies*.)
The query URL is:

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

Related concepts

Recommended settings and best practices on page 11
Redundancy and failover on page 6
Test your policies on page 9

Redundancy and failover

For each device you configure in the cloud portal, two Forcepoint points of presence (data centers or local PoPs) can be selected. Forcepoint strongly recommends configuring your device to achieve geographic redundancy using both PoP addresses.

> **Important**
>
> Connection redundancy is a requirement for the Forcepoint Web Security Cloud SLA

You can achieve geographic redundancy by either:

- Configuring primary and secondary tunnels, and using the connectivity monitoring address to monitor the status of the primary tunnel, with automatic failover to the secondary tunnel, or
- Configuring the two point of presence addresses as multiple IPsec peers for the same tunnel.

Use the appropriate IP addresses for your selected points of presence. These are listed in the article IP addresses for GRE and IPsec Advanced connectivity.

To decide which points of presence are best for your environment, consider:

- Which are nearest
- Any geographical or data sovereignty concerns around where users browse or where their reporting data is stored.

> **Note**
>
> Failover behavior, particularly cross-point of presence failover, could change an end user’s browsing experience. For example, some sites may change localization or presentation between a UK PoP and a German PoP (for example, www.google.co.uk might automatically redirect to www.google.de or www.google.nl, depending on which point of presence users’ traffic is directed though).
>
> Bear in mind that point of presence failover should be an exceptional occurrence, so this behavior might be acceptable in emergency circumstances.

Next steps

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)
- *Using single sign-on*
- 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*.

Related concepts

Enable notification pages for HTTPS sites on page 7
Set up end-user authentication on page 7
Configure browsers for NTLM identification on page 8
Using single sign-on on page 9
Test your policies on page 9

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.

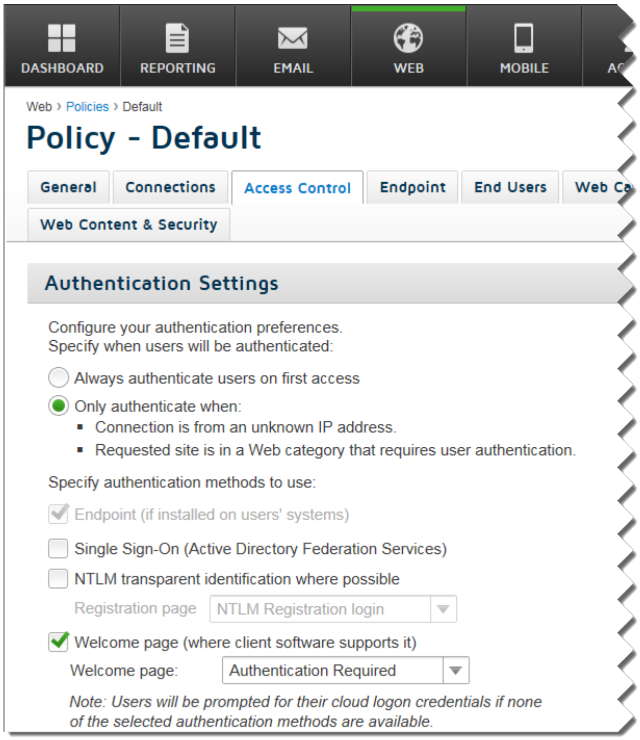
The setting is found on the **Web** > **Block & Notification Pages** page, under **Settings**. To enable it, select the checkbox **Use certificate to serve notifications for HTTPS pages**.

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 Advanced 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 cloud portal, used to define your authentication settings.



Policy - Default

Authentication Settings

Configure your authentication preferences.
Specify when users will be authenticated:

○ Always authenticate users on first access
● Only authenticate when:
- Connection is from an unknown IP address.
- Requested site is in a Web category that requires user authentication.

Specify authentication methods to use:

☑ Endpoint (if installed on users' systems)
☐ Single Sign-On (Active Directory Federation Services)
☐ NTLM transparent identification where possible
Registration page: NTLM Registration login
☑ Welcome page (where client software supports it)
Welcome page: Authentication Required

Note: Users will be prompted for their cloud logon credentials if none of the selected authentication methods are available.

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*.

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.

Related concepts
Limitations on page 12

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
```

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

Using single sign-on

Single sign-on using the SAML standard is supported for IPsec Advanced tunneling.

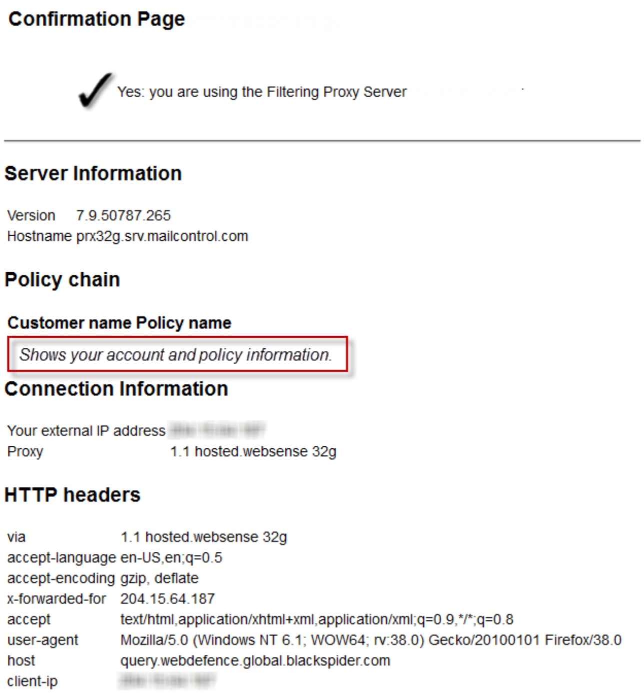
Single sign-on must be configured in the cloud portal. See Configure Single Sign-On settings in the cloud portal Admin Guide for more information.

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 prx32g.srv.mailcontrol.com
```

Policy chain

Customer name Policy name

Shows your account and policy information.

Connection Information

```
Your external IP address [redacted]
Proxy                    1.1 hosted.websense 32g
```

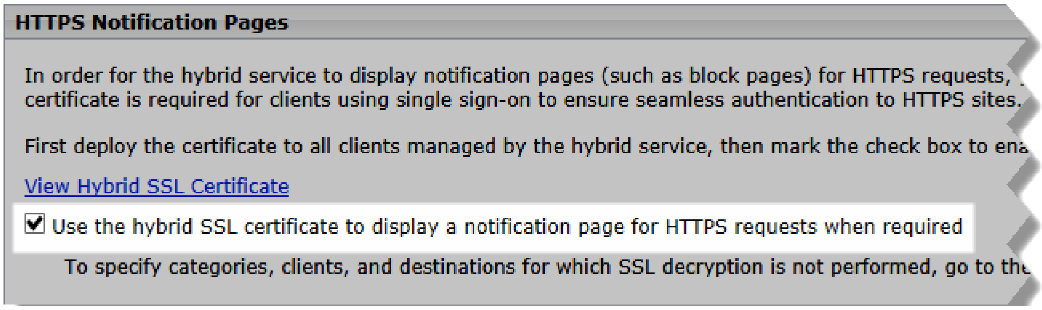
HTTP headers

```
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       [redacted]
```

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*.
- 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.



HTTPS Notification Pages

In order for the hybrid service to display notification pages (such as block pages) for HTTPS requests, certificate is required for clients using single sign-on to ensure seamless authentication to HTTPS sites.

First deploy the certificate to all clients managed by the hybrid service, then mark the check box to ena

View Hybrid SSL Certificate

☑ Use the hybrid SSL certificate to display a notification page for HTTPS requests when required

To specify categories, clients, and destinations for which SSL decryption is not performed, go to the

Related tasks

IP-based policy enforcement in hybrid deployments on page 10

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.

Recommended settings and best practices

The following tunnel negotiation and encryption settings are supported for IPsec Advanced. Recommended settings are shown in **bold**.

Setting	Supported (recommended settings in bold)
IKE version	**IKEv2** IKEv1
IKE cipher	**AES-128** **AES-256**
IKE message digest	**SHA2** SHA1
DH groups	**14** **19** 2 5
IPsec type	ESP
IPsec cipher	**AES-GCM-128** **AES-GCM-256** AES-128 AES-256 Null
IPsec message digest	**SHA2** SHA1
Authentication method	PSK only

Setting	Supported (recommended settings in bold)
IKE lifetime	24 hours
IPsec lifetime	8 hours
Perfect Forward Secrecy (PFS)	No

Forcepoint recommends the following best practices when configuring your IPsec solution:

- For devices with dynamic IP addresses, you must use IKEv2, using the DNS hostname as the IKE ID.
- Traffic routing: Forcepoint IPsec Advanced 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.
- If your IPsec edge device is behind another device in your network that is performing network address translation (NAT), NAT-traversal (NAT-T) must be enabled on your IPsec edge device.

Maximum Segment Size

The encapsulation overhead of the IPsec Advanced 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 points of presence 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.

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.

Limitations

The following items are known limitations of the Forcepoint IPsec Advanced solution.

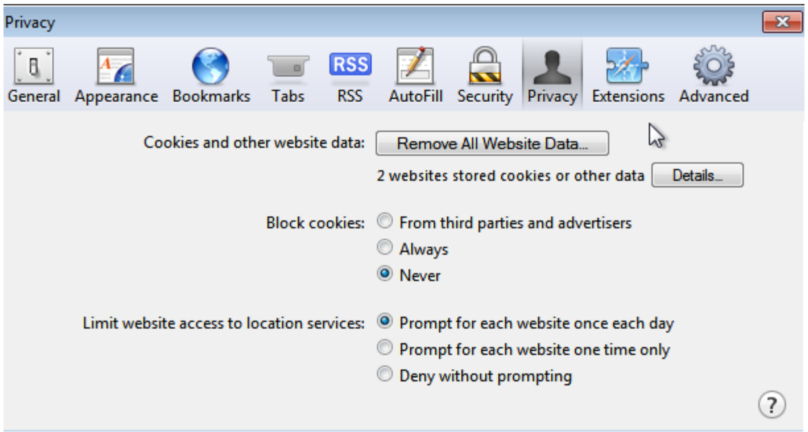
- Certificate authentication is not currently supported for IPsec Advanced.
- Forcepoint Web Security Endpoint is not supported for use with Forcepoint IPsec Advanced.
- Secure form-based authentication is not supported for use with Forcepoint IPsec Advanced.
- To support PAC file enforcement, you must use the alternate (port 80/443) PAC file address. The standard PAC file address (using port 8082/8087) is not supported.

- If a user has previously authenticated within the tunnel and relevant cookies are set, then using an authentication bypass rule to force NTLM, basic authentication, or a welcome page for a destination URL does not work with IPsec Advanced tunneling. However, if the first request is made to the URL configured under an authentication bypass rule, the selected authentication method in the rule will be enforced.
- Basic authentication does not work for iTunes with IPsec Advanced tunneling.
- SNI is required for HTTPS traffic when using transparent proxy.
  - Windows XP does not support SNI and is, therefore, not supported for Forcepoint IPsec Advanced.
  - Encrypted Client Hello (aka Encrypted SNI) is not supported when using transparent proxy.
- Dropbox is not supported for use with the Protected Cloud Apps feature in Forcepoint Web Security Cloud with IPsec Advanced.
- 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 Advanced 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:



Cookies and other website data: Remove All Website Data...

2 websites stored cookies or other data

Block cookies: ○ From third parties and advertisers
○ Always
● Never

Limit website access to location services: ● Prompt for each website once each day
○ Prompt for each website one time only
○ Deny without prompting

Troubleshooting

The following table lists some problems that may be encountered in configuring and establishing your tunnel, with some suggested actions.

Problem	Suggested actions
No traffic is reaching the cloud service	Check the tunnel status in the cloud portal, on the **Web** > **Device Management** page. This page gives an indication of the visibility of your tunnels to the cloud service.

Problem	Suggested actions
Your tunnel cannot be established	Use the appropriate `show` command for your device to display the tunnel status. If the tunnel is down, check the settings for your tunnel against the recommended settings detailed in the article IPsec configuration settings. Check that the following items have been correctly configured in your device's connection profile: ■ Connection IP address ■ Pre-shared key ■ IKE protocol ■ IKE cipher ■ IKE ID ■ IKE ID DH group ■ IPsec encryption algorithm In the cloud portal, check that the device's egress IP is configured correctly.
Your tunnel is up, but traffic is not flowing through the tunnel	Use the appropriate `show` command for your device to display the tunnel status. If the tunnel is up: ■ Verify that the tunnel connectivity monitoring address (116.50.59.230) can be pinged via the tunnel. ■ Check that the IPsec policy is configured to allow port 80 and 443 traffic through the tunnel. ■ If the edge device supports issuing an HTTP request via a utility such as curl or Wget, check that you can successfully receive an HTTP response from the proxy. ■ Capture traffic on the edge device and check if the traffic is being routed through the tunnel.

Problem	Suggested actions
Your device has previously connected, but cannot re-establish the tunnel	Check the settings for your tunnel against the recommended settings detailed in *Recommended settings and best practices*. 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.
Your tunnel has successfully established, but your policy settings are not being applied	Use the proxy query page to identify which policy is being applied. If necessary, revisit your policy settings. See *Test your policies*.
The policy test page is showing the correct policy, but some HTTPS connections are being closed. (HTTP requests are working.)	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*.
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*. Check your NTLM settings. See *Set up end-user authentication* and *Configure browsers for NTLM identification*. Ensure that your directory synchronization has successfully imported users and groups.
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*.

If you continue to have issues after checking all the items above, please contact Technical Support.

Related concepts

Recommended settings and best practices on page 11
Test your policies on page 9
Enable notification pages for HTTPS sites on page 7
Set up end-user authentication on page 7
Configure browsers for NTLM identification on page 8

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.

Published 12 August 2024