Cloud Web Security Service: VPN/IPsec Access Method

The AT&T Cloud Web Security Service solutions provide real-time protection against web-borne threats. As a cloud-based product, the Cloud Web Security Service leverages proven security technology, including the WebPulse™ cloud community.

With extensive web application controls and detailed reporting features, IT administrators can use the Cloud Web Security Service to create and enforce granular policies that are applied to all covered users, including fixed locations and roaming users.

This document describes how to configure a firewall/router device to send web traffic to the Cloud Web Security Service for security scanning and policy checks.

Table Of Contents

Cloud Web Security Service: VPN/IPsec Access Method .................................................................................. 3
   Table Of Contents ........................................................................................................................................ 3

Connectivity—About Virtual Private Network (IPsec) .................................................................................... 5
   Advantages of IPSec VPN Tunnels ............................................................................................................... 5
   IPSec Pre-deployment Considerations ....................................................................................................... 5
   About Supported VPN Tunnel Methods ..................................................................................................... 6
      Why Select This Method? ......................................................................................................................... 7
      Example .................................................................................................................................................. 9
      Why Select This Method? ......................................................................................................................... 9
      Scenario One—No Default Route, No On-Premises Proxy .................................................................. 10
      Scenario Two—Web Security Service as a Backup to an On-premises Proxy .................................. 10

Connectivity: VPN Pre-Shared Key with Static IP ......................................................................................... 12
   Technical Requirements ............................................................................................................................. 12
   Procedure—Establish a VPN Connection .................................................................................................... 13

Connectivity: VPN IKEv2 with Pre-Shared Key and Dynamic IP/FQDN ...................................................... 19
   Technical Requirements ............................................................................................................................. 19
   Procedure—Establish a VPN Connection .................................................................................................... 20
   Known Issue .............................................................................................................................................. 29

Connectivity: VPN Certificate Authentication .............................................................................................. 30
   Technical Requirements ............................................................................................................................. 30
   Blueprint Configuration—Configure Certificate Authentication for VPN Connection(s) .................... 31
# Connectivity: Explicit Over IPsec

## Technical Requirements

## Procedure

### Step 1—Configure a VPN Connection to the WSS

### Step 2—Configure Client Browsers to Explicit Proxy to the VPN Device

- **Example PAC File**

## Common Troubleshooting Tips

---

## Forward Specific User and Group Names to the Service

## Procedure

---

## Verify Connections

### Remote Users

- **Windows (UA)**
- **Mac (UA)**

---

## Reference

- **Reference: Cloud Web Security Service Data Center Ingress IPs**
- **Reference: Egress IP Ranges**
- **Reference: Required Locations, Ports, and Protocols**
  - **Symantec Resource**
  - **Access Methods**
  - **Authentication**
  - **Cloud-to-Premises DLP**
- **Reference: IKE Encryption and Authentication Algorithms**
- **Reference: Authentication IP Addresses**
- **About the All Ports License**

---

## Solve a Problem

- **Troubleshoot IPsec/VPN/Firewall Connections**
- **Stop Sending Traffic from a Location**
Connectivity—About Virtual Private Network (IPsec)

This topic provides details to help you build a robust, fault tolerant IPSec deployment for the AT&T Cloud Web Security Service (WSS). The configurations explained in this section are essential for a successful deployment and to ensure that your organization enjoys the maximum uptime per your Service Level Agreement (SLA).

Each section linked from this topic provides a set of technical requirements that go beyond simple best practices. For example, it is critical that your sites are configured with at least one backup tunnel to a secondary data center. Failure to configure a backup tunnel or adhere to other configuration recommendations will increase the likelihood of service issues as well as invalidate relevant SLA claims.

With the Firewall/VPN access method found in the location settings in the Cloud Web Security Service portal, you configure your web gateway firewall or router (referred to from here on as VPN device) to send the web traffic to the AT&T Cloud Web Security Service via an IPSec VPN tunnel for policy compliance and security.

**Warning:** It is essential that all recommendations in this guide be implemented, without exception, prior to your production deployment.

Advantages of IPSec VPN Tunnels

IPSec VPN tunnels provide confidentiality, data-integrity, data origin authentication and anti-replay protection for the traffic sent to the WSS by encapsulating WSS traffic in a virtual tunnel from your network’s edge to a WSS data center.

This type of configuration provides the following benefits:

- Does not require an agent on the client device.
- Client IP addresses are preserved for policy, authentication, and reporting.
- Confidentiality is achieved through the use of encryption algorithms, such as AES-256 and HMAC-SHA256, to encrypt the traffic sent over the IPSec tunnel to the WSS.
- Anti-replay protection that is built into the IPSec protocol protects against someone replaying IP packets sent to the WSS. (See complete list of algorithms supported by AT&T for IPSec connections in each of the blueprint configuration topics linked below).

IPSec Pre-deployment Considerations

Before you configure your VPN device to connect to the WSS, consider the following points:

- VPN Tunnel redundancy.

  In the extremely rare event that the connection to your primary WSS data center fails, your VPN device is responsible for diverting your web traffic to a backup WSS data center by way of a secondary VPN tunnel.

- IPSec does not permit stateful failover.
For most web applications, this is not a problem. However, clients using streaming media and conferencing applications may experience a brief disruption as your VPN device initiates your backup VPN tunnel.

- The Cloud Web Security Service is best suited to handle traffic destined for standard web resources.

  If your organization handles traffic that you do not want to send to the WSS, (such as Voice over IP, or private Intranet traffic) you must ensure that your firewall is configured to bypass that traffic.

- The Web Security Service supports up to to 500 mb/s of bandwidth per IPSec tunnel.

  Exceeding this limitation may result in performance issues. If you're unsure how to split traffic between multiple public IPs exiting your network, contact AT&T support for assistance.

  **Note:** You can send non-web traffic the WSS if you have the VPN All Ports license, but your security policies are not subjected to non-web traffic. See "About the All Ports License" on page 59.

IPSec supports two modes: Transport mode and Tunnel mode. WSS supports Tunnel mode using ESP (Encryption Security Payload) packets only. Interesting traffic, as defined in your VPN device, is encapsulated and sent inside the tunnel using ESP packets.

IPSec tunnel endpoints must authenticate each other before they exchange packets. This is done using the Internet Key Exchange (IKE) protocol. WSS supports both IKE version 1 (IKEv1) and IKE version 2 (IKEv2), but only under the conditions detailed under VPN Method Overviews, below.

WSS supports three different options to configure your VPN device to send traffic through IPSec VPN tunnels. This topic provides conceptual information to help you determine which is the most appropriate for your network, then provides links to topics that provide best practice guidance for configuring your IPSec VPN tunnels.

- If you know what deployment you require, select a link to the best practices topic.
  - "Connectivity: VPN Pre-Shared Key with Static IP" on page 12
  - "Connectivity: VPN IKEv2 with Pre-Shared Key and Dynamic IP/FQDN" on page 19
  - "Connectivity: VPN Certificate Authentication" on page 30

- In addition to the three IPSec configurations supported by WSS, there is also a deployment mode that tunnels explicit proxy connections over the IPSec site-to-site tunnel to WSS. This deployment method can be used with any of the IPSec configuration types described above.
  - "Connectivity: Explicit Over IPSec" on page 38

- If you need to understand the methods before deciding, continue reading the following sections.

**About Supported VPN Tunnel Methods**

Expand the following sections to learn more about each supported VPN connection method.
VPN Sites with Public IPs That Use Pre-Shared Key for Authentication

This method requires that your organization have a static public IP address, which is used to identify the location the VPN tunnel is connecting from. Locations are used to identify the account associated with a given connection in order to apply policy. This connection type does not support traversing a NAT device; connections must be initiated by an edge VPN device using one or more public IP addresses.

Why Select This Method?

Benefits—

- Requires no changes to desktops or servers.
- Authentication and redirection are transparent to end users.
- Web requests are redirected to the Cloud Web Security Service regardless of the originating application on the end user device.
- Supports client IP-based policy.
- Provides fully secured traffic between your site and the WSS.

Select another method if—

- Your network egress IP address is not static or the VPN device establishing your IPSec tunnel traverses a NAT device to access the Internet.

✓ Is this the method you require?

- For VPN sites that have static Public IPs and use a Pre-Shared Key for authentication, see "Connectivity: VPN Pre-Shared Key with Static IP" on page 12 for settings and best practices.
VPN Sites with Dynamic IPs that use FQDN for Identification and Pre-Shared Key (PSK) Authentication

Select this method if your site does not have a static IP address, such as when your VPN device is behind a NAT device. In this configuration, your VPN device is configured with a fully qualified domain name (FQDN) that it sends while establishing the VPN tunnel. The Cloud Web Security Service uses this FQDN to identify your location and assign policy accordingly.

**Note:** The FQDN does not need to be resolvable. There can be multiple devices with different FQDNs behind a single NAT device connecting through IPSec to the WSS.

☑ Is this the method you require?

- For VPN sites that can have dynamic IPs, use FQDN for identification, and Pre-Shared Key (PSK) authentication. See "Connectivity: VPN IKEv2 with Pre-Shared Key and Dynamic IP/FQDN" on page 19 for settings and best practices.
VPN Sites with Dynamic IPs that use Certificates for Identification and Authentication

This method is useful when your VPN appliance is not at the edge of your network and must traverse another device that obscures the source IP address (known as Network Address Translation Traversal or NAT-T).

Example

Picture a scenario where you are one of many aggregated businesses in a shopping mall. Each business relies on the property infrastructure to be their ISP. Rather than using your public IP address or FQDN, this method presents a unique certificate to the WSS that associates the VPN connection with your portal account.

Unlike other types of connection, you create this type of location by calling a WSS portal API that returns a one-time password (OTP). Your firewall uses that OTP to request to download a unique certificate from AT&T’s SCEP service.

Why Select This Method?

- There are multiple firewalls behind the NAT device, which prevents the use of a unique gateway IP address.
- When the PSK method is not possible when you do not manage the gateway device and the public-facing IP address.

✅ Is this the method you require?

- For VPN sites that can have dynamic IPs and use certificates for identification and authentication, see "Connectivity: VPN Certificate Authentication" on page 30 for settings and best practices.
Explicit Proxy Over IPsec

This deployment can be used with any of the IPSec location types supported by the Cloud Web Security Service. Use this method in environments where end user devices will not leverage the default route to connect transparently to the WSS, or when the Cloud Web Security Service will be used as a backup to an explicit on-premises proxy configuration. When active, end user browsers redirect traffic to the cloud proxy in WSS via the IPSec tunnel. To simplify the deployment of explicit proxy settings to end user devices, use a Proxy PAC file to automatically configure client browsers to point to the Cloud Web Security Service.

Tip: This method was previously referred to as Trans-Proxy.

Scenario One–No Default Route, No On-Premises Proxy

In network topologies where a default route to the internet does not exist (for example, sites that use Interior Gateway Protocol (IGP)), you can configure your users' browser's explicit proxy settings to route all web requests to the Cloud Web Security Service explicit proxy address: ep.threatpulse.net:80.

This explicit connection sends both HTTPS and HTTP over port 80 to the Cloud Web Security Service.

Data Flow

1. A client performs a web request (port 80).
   The browser's explicit proxy settings contain an explicit proxy hostname or IP address for the WSS, which is available through the IPSec tunnel.

2. The VPN device routes the request into the IPSec tunnel.

3. The Cloud Web Security Service receives the request, downloads the requested content, applies policy, and returns that content or a policy verdict to the requesting end user device inside the company network.

Scenario Two–Web Security Service as a Backup to an On-premises Proxy

When the primary proxy is an on-premises device (such as a ProxySG appliance) and the Cloud Web Security Service acts as a backup proxy, the PAC file used to configure client browsers should have the first entry point to the local on-premises proxy and a second entry point to the Cloud Web Security Service at ep.threatpulse.net:80.

Data Flow–WSS Backs Up Explicit Proxy Device

1. A client performs a web requests (port 80) and the on-premises proxy is not available.

2. The client browser or proxy-aware application fails over to the second PAC file entry for ep.threatpulse.net:80.

3. The edge VPN device routes the request into the IPSec tunnel.
4. The Cloud Web Security Service receives the request and downloads the requested content, applies policy, and returns that content or a policy verdict to the requesting end user device inside the company network.

✔️ Is this the method you require?

Connectivity: VPN Pre-Shared Key with Static IP

This method is configuring a VPN tunnel to connect to the Cloud Web Security Service using IKEv1 and a pre-shared key (PSK) for site-to-site authentication. The method requires that your organization have a static public IP address. That IP address is used to identify your site when it connects to the WSS.

AT&T uses industry standard strong encryption algorithms, including AES-256, to ensure all traffic is kept private as it passes to the WSS. During configuration, you specify a pre-shared key for the VPN tunnel. This enables more control of the security of the IPsec tunnel, as you can change the key as needed to fit any company or compliance requirement.

Technical Requirements

This section provides a high-level set of technical requirements for this perform this configuration.

- Your organization has been provisioned with an account in the WSS.
  
  To confirm this, browse to [https://portal.threatpulse.com](https://portal.threatpulse.com) and log in. If you are unable to log in, verify your account details with AT&T support.

- If you are not certain what type of connection is appropriate for your organization, see "Connectivity—About Virtual Private Network (IPsec)" on page 5.

- An understanding of how much user traffic will route to the Cloud Web Security Service.
  
  The WSS is limited to 500mbit/s of bandwidth per IPSec tunnel. If you expect traffic to exceed that, you must plan your architecture to use an additional tunnel from an additional public IP address for each 500mbit/s block of bandwidth you expect to consume. For example, if one of your sites consumes 900mbit/s of traffic, it must connect to the WSS using at least two IPsec tunnels, each connecting from a unique public IP address. If you are not sure how to configure your VPN device to split traffic in this way, please contact AT&T support.

- The following information is required to ensure a successful configuration.
  
    - Your site's public IP address.
    - Your closest two data center addresses configured for failover to your site.
    - A list of intranet destinations to exclude from the IPsec VPN tunnel(s).
    - Ensure that your IPsec VPN device supports Dead Peer Detection. This feature ensures that if a connection fails, that failure is detected and the secondary tunnel is used.
      
        - In the event that your VPN device supports IPSLA (Internet protocol service level agreement) and DPD, AT&T suggests that you configure both to ensure maximum uptime.
      
      - Your network’s edge firewall is configured to permit the necessary traffic outbound for IPsec connections: ports 88/443; UDP port 500; and UDP port 4500.

For additional ports and URLs used in a connection between your network and the WSS, see "Reference: Required Locations, Ports, and Protocols" on page 51.
Each VPN device vendor manages this differently, but the focus is to define what traffic on your internal network will be encrypted and sent through the tunnel. In most cases, this is done with an Access Control List (ACL) that includes the data ports (typically, TCP ports 80 and 443) and your user subnets, and excludes intranet servers and services.

Procedure—Establish a VPN Connection

A complete VPN configuration requires some configuration both in the portal and your on-premises VPN device.

Create a Location in the Portal

First, you create a fixed Location in the WSS portal. A Location instructs the WSS to accept incoming connections from the VPN device’s IP address.

1. Log in to your WSS portal. In Service Mode, select Network > Locations.
2. Click Add Location.
3. Enter the Location and security information.

a. The Name of the location. For example, the geo-physical location or office name.

b. Select Firewall/VPN as the Access Method.
c. Enter the Gateway IP address; the public IP address of your network.

d. Define the Authentication Key (pre-shared key) used to authenticate communication from the router.

4. Enter resource and location information.

<table>
<thead>
<tr>
<th>Estimated Users:</th>
<th>51 to 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country:</td>
<td>United States</td>
</tr>
<tr>
<td>Time Zone:</td>
<td>Pacific Time (Amer</td>
</tr>
<tr>
<td>Address Line 1:</td>
<td>1 Shark Tank Way</td>
</tr>
<tr>
<td>Address Line 2:</td>
<td>San Jose, CA</td>
</tr>
<tr>
<td>Zip / Postal Code:</td>
<td>95111</td>
</tr>
<tr>
<td>Comments:</td>
<td>Router that serves all senior executive offices.</td>
</tr>
</tbody>
</table>

a. Select the Estimated User range that represents the number of users behind your VPN device accessing the internet through WSS.

b. (Optional) Select a Time Zone, fill out location information, and enter comments (optional).

c. (Optional) Complete location information.

5. Click Save.

Blueprint—Create a Connection in the VPN Device

If the example configurations in the previous section do not closely match your VPN device, refer to the following required configurations.
1. Define interesting traffic.

Each VPN device vendor manages this differently, but the focus is to define what traffic on your internal network will be encrypted and sent through the tunnel. In most cases, this is done with an Access Control List (ACL) that includes the data ports (typically, TCP ports 80 and 443) and your user subnets, and excludes intranet servers and services.

2. Configure the IKE Phase 1 details.

The first phase of the Internet Key Exchange is to establish a connection through which your data will be tunneled. While Main and Aggressive mode options are present on most VPN devices, the WSS supports Main mode only. Aggressive mode is supported in certain circumstances, but only as directed by AT&T support personnel.

IKE Phase 1 includes the following parameters:

- **Destination address.**
  
  Set the VPN destination address as the closest WSS Data Center to your location. A list of Data Center addresses—
  

- **Internet Key Exchange (IKE) ID.**

  Set the public IP address (or FQDN, if your public IP address is not static) as its IKE ID.

- **IPsec Lifetime.**

  The IPSEC lifetime determines when the phase 2 tunnel expires. This can be specified both in terms of time and is terms of bytes or packets transferred. WSS recommends using time only. VPN devices should be configured to re-establish a new tunnel with new encryption keys before an existing phase 2 tunnel expires - this process is called rekeying.

  The time configured should be more than 1 hour (3600 seconds) and less than the Phase 1 lifetime. AT&T recommends this value to be 4 hours.

**Notes:**

- IKEv1 allows negotiation of a lifetime between the two sides. WSS will not expire a tunnel before the other side (your VPN device).

- IKEv2 does not allow negotiation of a lifetime and each side is free to choose its one time for expiring a tunnel. Currently, WSS uses 1 hour for its Phase 2 (IPSec) IKEv2 tunnel. To ensure maximum uptime, AT&T requires that you configure your VPN device to use a value slightly less than 1 hour and allow re-key of the tunnel before expiry of the tunnel.

- **Pre-Shared Key (PSK)**

  Define this as you did in the portal. If these values fail to match, the connection does not establish.

- **Diffie-Hellman (DH) Exchange.**

  This value is used by both ends to exchange matching shared secret keys, used to secure the tunnel between your VPN device and WSS for phase 2. The following table provides the DH groups supported by the WSS.
Encryption Algorithm—This is the type of encryption used to secure the data exchanged between your VPN device and WSS. The following values are supported:

<table>
<thead>
<tr>
<th>Encryption Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keyword</strong></td>
</tr>
<tr>
<td>aes128</td>
</tr>
<tr>
<td>aes256</td>
</tr>
<tr>
<td>aes192ct</td>
</tr>
<tr>
<td>aes128ccm8</td>
</tr>
<tr>
<td>aes256ccm8</td>
</tr>
<tr>
<td>aes192ccm12</td>
</tr>
<tr>
<td>aes128ccm16</td>
</tr>
<tr>
<td>aes256ccm16</td>
</tr>
<tr>
<td>aes192ccm16</td>
</tr>
<tr>
<td>aes128gcm8</td>
</tr>
<tr>
<td>aes256gcm8</td>
</tr>
<tr>
<td>aes192gcm12</td>
</tr>
<tr>
<td>aes128gcm12</td>
</tr>
<tr>
<td>aes256gcm12</td>
</tr>
<tr>
<td>aes192gcm16</td>
</tr>
<tr>
<td>aes128gmac</td>
</tr>
<tr>
<td>aes256gmac</td>
</tr>
<tr>
<td>blowfish128</td>
</tr>
<tr>
<td>blowfish256</td>
</tr>
<tr>
<td>camellia192</td>
</tr>
</tbody>
</table>

Dead Peer Detection (DPD)—Depending on your VPN device and network configuration, AT&T recommends that DPD is set to check every thirty seconds with five retries. The following is a known list of common vendor instructions for DPD:

- Cisco Router info for DPD- [Cisco Routers DPD](#)
- Cisco Community DPD Article- [Cisco DPD Info](#)
- Checkpoint DPD Info - [Checkpoint KB on DPD](#)
Firewall/VPN Access

- Juniper DPD - [Juniper DPD Info](#)
- Palo Alto DPD - [Palo Alto DPD KB](#)
- Fortinet Fortigate DPD - [Fortigate DPD](#)
- If your manufacturer is not listed, consult their website or support team for assistance with this feature.

**IPsec Anti-Replay**

This option prevents a man-in-the-middle attack by detecting if any packets have been sent or received already. If there have been, the connection is broken and re-established. Some amount of retransmitted traffic is expected; therefore, it is important to set this has a value that provides the best security and flexibility. AT&T recommends setting the window to 32.

3. Configure the IKE Phase 2 details.

The second phase of the Internet Key Exchange is used to negotiate IPsec Security Associations (SAs) to set up the IPsec tunnel.

- For Phase 2, AT&T recommends the timeout be 4 hours or less to avoid split protocol and other connection issues.
- Associate your interesting traffic ACL with this configuration.
- Enable Perfect Forward Secrecy (PFS).
- Network Address Translation.

  Disable this option. This ensures that all traffic from your users reaches the WSS with its original source IP address. Failing to observe this can lead to users not being authenticated, or to policy rules not applying to traffic as expected.

4. Save the VPN configuration, and repeat this process with the data center that is the next closest to your geographic location.

**Helpful Tips**

The following knowledge base articles cover information that can be useful in troubleshooting issues once the VPN tunnel is established.

- Data Center Egress IP Addresses. The following articles provide the public IP addresses used to reach Internet resources from the Cloud Web Security Service worldwide:

Browser Error on IPsec VPN if First Request is HTTPS: [https://support.symantec.com/en_US/article.TECH246221.html](https://support.symantec.com/en_US/article.TECH246221.html)

VPN Device Reference Configurations

The following links provide example vendor device configuration examples. Use these as *guidelines only*. AT&T cannot guarantee the validity of third-party products and procedures. If you encounter configuration discrepancies, you must default to the best practices and configuration parameters provided by AT&T in this topic. Per the SLA, Technical Support might not be able to provide guidance if you perform configurations outside of the requirements outlined in this guide.

**Note:** VPN device vendors routinely change user interfaces; however, the required VPN-to-VPN settings rarely change.


Next Selection

- IPsec deployment: Proceed to "Verify Connections" on page 43.

- Explicit Over IPsec deployment: Add the explicit proxy entry to PAC file. See "Connectivity: Explicit Over IPsec" on page 38.
Connectivity: VPN IKEv2 with Pre-Shared Key and Dynamic IP/FQDN

This method is configuring a VPN tunnel to connect to the Cloud Web Security Service using IKEv2 with a fully qualified domain name (FQDN) and a pre-shared key (PSK) for site-to-site authentication. This method is appropriate if your network does not have a static IP address or if your VPN tunnel is initiated behind a device that performs Network Address Translation (NAT).

AT&T uses industry standard strong encryption algorithms, including AES-256, to ensure all traffic is kept private as it passes to the WSS. During configuration, you specify an FQDN to identify your site and a pre-shared key for authentication. You can choose a pre-shared key that fits your company’s compliance requirement. The FQDN and pre-shared key can be changed from the WSS portal if and when needed; however, a change results in the tunnel re-establishing. Note that the WSS does not resolve the FQDN.

Technical Requirements

This section provides a high-level set of technical requirements for this configuration.

- Your organization has been provisioned with an account in the WSS.
  
  To confirm this, browse to https://portal.threatpulse.com and log in. If you are unable to log in, verify your account details with AT&T support.

- If you are not certain what type of connection is appropriate for your organization, see “Connectivity—About Virtual Private Network (IPsec)” on page 5.

- An understanding of how much user traffic will route to the Cloud Web Security Service.

  The WSS is limited to 500mbit/s of bandwidth per IPSec tunnel. If you expect traffic to exceed that, you must plan your architecture to use an additional tunnel from an additional public IP address for each 500mbit/s block of bandwidth you expect to consume. For example, if one of your sites consumes 900mbit/s of traffic, it must connect to the WSS using at least two IPSec tunnels, each connecting from a unique public IP address. If you’re not sure how to configure your VPN device to split your traffic between multiple connections, please contact AT&T support for assistance.

- The following information is required to ensure a successful configuration.
  
  - Your network’s fully qualified domain name (FQDN) for authentication.
  - The two closest data center IP addresses.

    All VPN configurations must include a primary and secondary tunnel to the WSS. If one data center connection becomes unavailable, your site’s traffic can be routed to a secondary tunnel to another data center. See "Reference: Cloud Web Security Service Data Center Ingress IPs" on page 49 for geographical IP address information.

  - A list of intranet destinations to exclude from the IPsec VPN tunnel(s).

    For example, as a best practice do not send intranet resources, such as email and internal web services, through the tunnel. Additionally, exclude the server where the Auth Connector is installed from the tunnel as it makes a direct connection to the WSS through port 443. See "Forward Specific User and Group Names to the Service" on page 41.
Ensure that your IPsec VPN device supports **Dead Peer Detection**. This feature ensures that if a connection fails, that failure is detected and the secondary tunnel is used.

- If your VPN device supports IPSLA (Internet protocol service level agreement) and DPD, AT&T suggests that you configure both to ensure maximum uptime.

- Your network edge firewall is configured to permit the necessary traffic outbound for IPsec connections: ports 80/443; UDP port 500; and UDP port 4500.

For additional ports and URLs used in a connection between your network and the WSS, see "Reference: Required Locations, Ports, and Protocols" on page 51.

**Procedure—Establish a VPN Connection**

**Create a Location in the Portal**

First, you create a *Location* in the WSS portal. A Location instructs the WSS to accept incoming connections from your VPN device’s FQDN.

1. Log in to your WSS portal. In Service Mode, select **Network > Locations**.
2. Click **Add Location**.
3. Enter the **Location** and security information.

```
<table>
<thead>
<tr>
<th>Add Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Name: <em>ExecTeam</em></td>
</tr>
<tr>
<td>Access Method: <em>FQDN IKEv2 Firewall</em></td>
</tr>
<tr>
<td>FQDN Address: <em>testgateway.example.com</em></td>
</tr>
<tr>
<td>Preshared Key: *************</td>
</tr>
</tbody>
</table>
```

- **a.** The Name of the location. For example, the geo-physical location or office name.
- **b.** Select **FQDN IKEv2 Firewall** as the Access Method.
c. Enter the **FQDN Address** that you will use for authentication.
d. Define the **Pre-Shared Key** used to authenticate the VPN tunnel from the router.

4. Enter resource and location information.

![Input fields for resource and location information]

- a. Select the **Estimated User** range that will be sending web requests through this gateway interface. AT&T uses this information to ensure proper resources.
- b. (Optional) Select a **Time Zone**, fill out location information, and enter comments (optional).
- c. (Optional) Complete location information.

5. Click **Save**.

**Blueprint—Configure a VPN Connection to the WSS**

If the example configurations in the previous section do not closely match your VPN device, refer to the following required configurations.
1. Decide the version of IKE (IKEv1 or IKEv2) to use.

   Not all VPN devices support IKEv2. Verify that your version of the device supports IKEv2.

2. IPSec VPN tunnel establishment has two phases and hence the configuration is usually made up of two sets of configuration.

   The terminology used to define the two phases differs from vendor to vendor and also differs based on the IKE version used. Phase1, ISAKMP, IKEv1, IKEv2 or IKE are some of the common terms used to refer to the class of configuration for the IKE tunnel (connection). The IKE tunnel is then used to setup the IPSec tunnel over which the actual data is transferred. Phase 2 and IPSec are some of the common terms used to refer to this class of configuration.

3. Define interesting traffic.

   Each VPN device vendor manages this differently, but the focus is to define what traffic on your internal network will be encrypted and sent through the tunnel. In most cases, this is done with an access control list (ACL) that includes the data ports (typically, TCP ports 80 and 443) and your user subnets, and excludes intranet servers and services.

4. Configure the IKE Phase 1 details.

   The first phase of IKE is to establish a secure connection over which further IKE exchanges happen. This phase authenticates each of the endpoint devices in the tunnel to each other. Phase 1 is also used to negotiate phase 2 tunnel parameters. IKEv1 supports two different modes for phase 1 - Main Mode and Aggressive mode. The WSS supports Main mode only. Aggressive mode is supported in certain circumstances, but only as directed by AT&T support personnel. IKEv2 has only one mode.

   IKE Phase 1 configuration includes the following parameters:

   - If using IKEv1, select Main Mode for configuration. There is only one mode for IKEv2.
   - When asked to select Tunnel or Transport type/mode of connection, select **Tunnel mode**.
   - Destination address.

     Set the VPN destination address as the closest WSS Data Center to your location. A list of Data Center addresses—


   - Internet Key Exchange (IKE) ID.

     IKE IDs are how each peer in the VPN tunnel identifies itself to the other side. There is a Local Identifier, which is the identifier for your device; and there is Remote Identifier, which is the identifier for the other side of the connection (Data Center in this case). The names might vary based on your device vendor.

     Set the Local Identifier to be the public IP address of your device. This is the IP that is used to create the location in the WSS Portal.

     Set the Remote Identifier to be the IP of the Data Center you are connecting to.

   - IKE Lifetime.
This lifetime determines the time when the Phase 1 tunnel is renegotiated. AT&T recommends this to be in hours. Commonly used values are 12 and 24 hours.

**Tip:** Many VPN devices expect the IKE lifetime value to be detailed in minutes. Consult your documentation to confirm.

- **Pre-Shared Key (PSK).**
  Define this as you did in the portal. If these values fail to match, the connection does not establish.

- **Encryption Algorithm Proposals**
  A proposal used to specify the encryption algorithm, the data integrity algorithms and the strength of the Diffie-Hellman (DH) exchange (defined by the group of the DH group). The initiator of the phase 1 (your VPN device) will send a list of one or more such proposals during the IKE handshake and WSS will choose one that it supports from this list. The two sides negotiate an encryption algorithm, a data integrity algorithm and a DH group that both sides support.

  After the handshake is completed successfully, a Security Association (SA) is setup between the two sides that uses this proposal that the two sides agree upon.

  The following text lists the different encryption algorithms, the data authentication mechanism and the DH groups supported by WSS.

- **Encryption Algorithm**—This is the type of encryption used to secure the data exchanged with between your VPN device and the Cloud Web Security Service. The following values are supported:

  ![Encryption Algorithms Table]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes128</td>
<td>128 bit AES-CBC</td>
<td>aes192</td>
<td>192 bit AES-CBC</td>
</tr>
<tr>
<td>aes256</td>
<td>256 bit AES-CBC</td>
<td>aes128ctr</td>
<td>128 bit AES-COUNTER</td>
</tr>
<tr>
<td>aes192ctr</td>
<td>192 bit AES-COUNTER</td>
<td>aes256ctr</td>
<td>256 bit AES-COUNTER</td>
</tr>
<tr>
<td>aes128ccm8</td>
<td>128 bit AES-CCM with 64 bit ICV</td>
<td>aes192ccm8</td>
<td>192 bit AES-CCM with 64 bit ICV</td>
</tr>
<tr>
<td>aes256ccm8</td>
<td>256 bit AES-CCM with 64 bit ICV</td>
<td>aes128ccm12</td>
<td>128 bit AES-CCM with 96 bit ICV</td>
</tr>
<tr>
<td>aes192ccm12</td>
<td>192 bit AES-CCM with 96 bit ICV</td>
<td>aes256ccm12</td>
<td>256 bit AES-CCM with 96 bit ICV</td>
</tr>
<tr>
<td>aes128ccm16</td>
<td>128 bit AES-CCM with 128 bit ICV</td>
<td>aes192ccm16</td>
<td>192 bit AES-CCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes256ccm16</td>
<td>256 bit AES-CCM with 128 bit ICV</td>
<td>aes128ccm16</td>
<td>128 bit AES-CCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes192ccm16</td>
<td>192 bit AES-CCM with 128 bit ICV</td>
<td>aes256ccm16</td>
<td>256 bit AES-CCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes128gcm12</td>
<td>128 bit AES-GCM with 96 bit ICV</td>
<td>aes192gcm12</td>
<td>192 bit AES-GCM with 96 bit ICV</td>
</tr>
<tr>
<td>aes256gcm12</td>
<td>256 bit AES-GCM with 96 bit ICV</td>
<td>aes128gcm12</td>
<td>128 bit AES-GCM with 96 bit ICV</td>
</tr>
<tr>
<td>aes192gcm12</td>
<td>192 bit AES-GCM with 96 bit ICV</td>
<td>aes256gcm12</td>
<td>256 bit AES-GCM with 96 bit ICV</td>
</tr>
<tr>
<td>aes128gcm16</td>
<td>128 bit AES-GCM with 128 bit ICV</td>
<td>aes192gcm16</td>
<td>192 bit AES-GCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes256gcm16</td>
<td>256 bit AES-GCM with 128 bit ICV</td>
<td>aes128gcm16</td>
<td>128 bit AES-GCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes192gcm16</td>
<td>192 bit AES-GCM with 128 bit ICV</td>
<td>aes256gcm16</td>
<td>256 bit AES-GCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes128gmac12</td>
<td>Null encryption with 128 bit AES-GMAC</td>
<td>aes192gmac12</td>
<td>Null encryption with 192 bit AES-GMAC</td>
</tr>
<tr>
<td>aes256gmac12</td>
<td>Null encryption with 256 bit AES-GMAC</td>
<td>aes128gmac12</td>
<td>Null encryption with 128 bit AES-GMAC</td>
</tr>
<tr>
<td>aes192gmac12</td>
<td>Null encryption with 192 bit AES-GMAC</td>
<td>aes256gmac12</td>
<td>Null encryption with 256 bit AES-GMAC</td>
</tr>
<tr>
<td>blowfish128</td>
<td>128 bit Blowfish-CBC</td>
<td>blowfish192</td>
<td>192 bit Blowfish-CBC</td>
</tr>
<tr>
<td>blowfish128</td>
<td>128 bit Blowfish-CBC</td>
<td>blowfish192</td>
<td>192 bit Blowfish-CBC</td>
</tr>
<tr>
<td>blowfish192</td>
<td>192 bit Blowfish-CBC</td>
<td>camellia192</td>
<td>192 bit Camellia-CBC</td>
</tr>
<tr>
<td>camellia256</td>
<td>256 bit Camellia-CBC</td>
<td>camellia192</td>
<td>192 bit Camellia-CBC</td>
</tr>
<tr>
<td>camellia256</td>
<td>256 bit Camellia-CBC</td>
<td>camellia192</td>
<td>192 bit Camellia-CBC</td>
</tr>
</tbody>
</table>
- Integrity Algorithms
  These algorithms are used to enforce the integrity of the data exchanged.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>MD5 HMAC</td>
<td>96 bit</td>
</tr>
<tr>
<td>sha1 or sha2_250</td>
<td>SHA1 HMAC</td>
<td>96 bit</td>
</tr>
<tr>
<td>sha256 or sha2_256</td>
<td>SHA2_256_128 HMAC</td>
<td>128 bit</td>
</tr>
<tr>
<td>sha384 or sha3_384</td>
<td>SHA2_384_192 HMAC</td>
<td>192 bit</td>
</tr>
<tr>
<td>sha512 or sha3_512</td>
<td>SHA2_512_256 HMAC</td>
<td>256 bit</td>
</tr>
</tbody>
</table>

  This value is used by both ends to exchange matching shared secret keys that are used to secure the tunnel between your VPN device and WSS.
  The following table provides the DH groups supported by the WSS:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>DH Group</th>
<th>Modulus</th>
</tr>
</thead>
<tbody>
<tr>
<td>modp1024</td>
<td>2</td>
<td>1024 bits</td>
</tr>
<tr>
<td>modp1536</td>
<td>3</td>
<td>1536 bits</td>
</tr>
<tr>
<td>modp2048</td>
<td>14</td>
<td>2048 bits</td>
</tr>
<tr>
<td>modp3072</td>
<td>15</td>
<td>3072 bits</td>
</tr>
<tr>
<td>modp4096</td>
<td>16</td>
<td>4096 bits</td>
</tr>
<tr>
<td>modp6144</td>
<td>17</td>
<td>6144 bits</td>
</tr>
<tr>
<td>modp8192</td>
<td>18</td>
<td>8192 bits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Modulo Prime Groups with Prime Order Subgroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>modp1024</td>
</tr>
<tr>
<td>modp2048</td>
</tr>
</tbody>
</table>

- Dead Peer Detection (DPD)—Ensure this option is enabled, and set to check every ten seconds with three retries.
  The following is a known list of common vendor instructions for DPD.
  - Cisco Router info for DPD- [Cisco Routers DPD](#)
  - Cisco Community DPD Article- [Cisco DPD Info](#)
  - Checkpoint DPD Info - [Checkpoint KB on DPD](#)
  - Juniper DPD - [Juniper DPD Info](#)
  - Palo Alto DPD - [Palo Alto DPD KB](#)
  - Fortinet Fortigate DPD - [Fortigate DPD](#)
  - If your manufacturer is not listed, consult their website or support team for assistance with this feature.
**Note:** Each VPN device vendor provides details specific to site-to-site VPN connections with their own devices only. In some cases, the values provided here may not provide the best experience. If you experience issues with dead peer detection on your tunnel connections with the WSS, contact AT&T support.

- **IPsec Anti-Replay**
  
  This option prevents a man-in-the-middle attack by detecting if any packets have been sent or received already. If they are, the connection is broken and re-established. Some amount of retransmitted traffic is expected; therefore it is important to set this as a value that provides the best security and flexibility. AT&T recommends setting the window to 32.

5. **Configure the IKE Phase 2 details.**

- **Phase 2 or IPSec Encryption Algorithm Proposals**
  
  Similar to Phase 1 proposals, a phase 2 proposal is used to specify the encryption algorithm, the data integrity algorithms and the strength of the Diffie-Hellman (DH) exchange (defined by the group of the DH group) for the IPSec tunnel on which the actual data (the data that needs to be protected by the WSS) is exchanged.

  For phase 2, an additional parameter may need to be configured. This is the protocol to be used for the IPSec encoding. There are two protocols defined by the standard—Encapsulating Security Payload (ESP) and Authentication Header (AH). WSS uses only ESP.

  The initiator of the Phase 2 handshake (your VPN device) sends a list of one or more such proposals during the handshake and the WSS selects the one that it supports from this list. The two sides thus negotiate an encryption algorithm, a data integrity algorithm, and a DH group that both sides support.

  After the handshake is completed successfully, an IPSec Security Association (SA) is setup between the two sides that uses this proposal that the two sides agree upon.

  The following text list the different encryption algorithms, the data authentication mechanism and the DH groups supported by WSS:
Note: Choosing DH Groups will also enable Perfect Forward Secrecy PFS (described below) in many VPN devices.

- PFS (Perfect Forward Secrecy)
Use of PFS increases security by protecting against compromises of encryption keys. AT&T recommends use of PFS.

- **IPSec Lifetime**

  The IPSEC lifetime determines when the phase 2 tunnel expires. This can be specified both in terms of time and is terms of bytes or packets transferred. AT&T recommends using time only. Your VPN devices should be configured to re-establish a new tunnel with new encryption keys before an existing phase 2 tunnel expires. This process is called re-keying.

  The time configured should be more than 1 hour (3600 seconds) and less than the Phase 1 lifetime. AT&T recommends this value to be 4 hours.

  **Note:** IKEv1 allows negotiation of a lifetime between the two sides. The WSS will not expire a tunnel before the other side (your VPN device).

  **Note:** IKEv2 does not allow negotiation of a lifetime and each side is free to choose its one time for expiring a tunnel. Currently, WSS uses 1 hour for its Phase 2 (IPSec) IKEv2 tunnel. AT&T recommends that you configure your VPN device to use a value of 55 minutes. This ensures the tunnel re-keys before it expires.

- **IPsec Anti-Replay.**

  This option prevents a man-in-the-middle attack by detecting if any packets have been sent or received already. If they are, the connection is broken and re-established. Some amount of retransmitted traffic is expected; therefore, it is important to set this has a value that provides the best security and flexibility. AT&T recommends setting the window to 32.

- **Network Address Translation.**

  Disable this option. This ensures that all traffic from your users reaches the WSS with its original source IP address. Failing to observe this can lead to users not being authenticated, or to policy rules not applying to traffic as expected.

- **NAT Traversal (NAT-T).**

  If your VPN device is behind NAT (the public IP is not on the device, but on a upstream router), then the following configuration changes are needed to make the tunnel work:

  - Enable NAT-T on the device, but configure the device to send the upstream public IP as its Local Identifier.
  - Disable NAT-T on the device (if this is supported).
6. Save the VPN configuration, and repeat this process to configure a secondary tunnel to a data center that is the next closest to your site.

Helpful Tips

The following knowledge base articles cover information that can be useful in troubleshooting issues once the VPN is established.


- Data Center Egress IP Addresses. The following articles provide the public IP addresses used to reach internet resources from WSS Data Centers worldwide:


- Browser Error on IPsec VPN if First Request is HTTPS: [https://support.symantec.com/en_US/article.TECH246221.html](https://support.symantec.com/en_US/article.TECH246221.html)

VPN Device Reference Configurations

The following links provide example vendor device configuration examples. Use these as guidelines only. AT&T cannot guarantee the validity of third-party products and procedures. If you encounter configuration discrepancies, you must default to the best practices and configuration parameters provided by AT&T in this topic. Per the SLA, Technical Support might not be able to provide guidance if you perform configurations outside of the recommendations.

Note: VPN device vendors routinely change user interfaces; however, the required VPN-to-VPN settings rarely change.


**Known Issue**

- IKEv2 tunnels.

  **ISSUE:** Child SAs (phase 2 tunnels) from IKEv2 FQDN sites expire one hour after the time of creation.

  **WORKAROUND:** To ensure that there is no loss of connectivity, configure the firewalls to have child SA (or phase 2) lifetime of less than an hour to ensure that a new SA is in place before the old SA expires.

  *(DP-310)*

**Next Selection**

- IPsec deployment: Proceed to "Verify Connections" on page 43.

- Explicit Over IPsec deployment: Add the explicit proxy entry to PAC file. See "Connectivity: Explicit Over IPsec" on page 38.
Connectivity: VPN Certificate Authentication

Also known as RSA-SIG, using certificate authentication (instead of a pre-shared key) to verify your network’s identity when connecting to Cloud Web Security Service is very secure. This method is ideal if your VPN device is behind a NAT device, as it does not rely on the external IP address or FQDN of your organization’s external IP.

Technical Requirements

This section provides a high-level set of technical requirements required for this configuration.

- Your organization has been provisioned with an account in the WSS, and you have successfully completed the registration of that account.

  To confirm this, browse to https://portal.threatpulse.com and log in. If you are unable to log in, verify your account details with AT&T support.

- If you are not certain what type of connection is appropriate for your organization, see “Connectivity—About Virtual Private Network (IPsec)” on page 5.

- An understanding of how much user traffic will route to the Cloud Web Security Service.

  The WSS is limited to 500mbit/s of bandwidth per IPSec tunnel. If you expect traffic to exceed that, you must plan your architecture to use an additional tunnel from an additional public IP address for each 500mbit/s block of bandwidth you expect to consume. For example, if one of your sites consumes 900mbit/s of traffic, it must connect to the WSS using at least two IPSec tunnels, each connecting from a unique public IP address. If you're not sure how to configure your VPN device to split your traffic between multiple connections, please contact AT&T support for assistance.

- The following information is required to ensure a successful configuration.

  - The public IP address or fully qualified domain name (FQDN).
  
  - The two closest data center addresses.

    All VPN configurations must include a primary and secondary tunnel to the WSS. If one data center connection becomes unavailable, your site’s traffic can be routed to a secondary tunnel to an alternate data center. See “Reference: Cloud Web Security Service Data Center Ingress IPs” on page 49 for geographical IP address information.

  - The internal network addresses that is the source of data to send to the WSS.

    For example, as a best practice do not send intranet resources, such as email and internal web services, through the tunnel. Additionally, exclude the server where the Auth Connector is installed from the tunnel as it makes a direct connection to the WSS through port 443. See "Forward Specific User and Group Names to the Service" on page 41.

  - A list of intranet destinations to exclude from the IPsec VPN tunnel(s).

  - Ensure that your VPN device supports Dead Peer Detection. This feature ensures that if the primary VPN tunnel fails, that failure is detected and the secondary tunnel is used.

    - If your VPN device supports IPSLA (Internet protocol service level agreement) and DPD, AT&T suggests that you configure both to ensure maximum uptime.

    - Your VPN device is configured to permit the necessary traffic outbound for IPsec connections. These are
destination UDP ports 500 and 4500, and also packets of type ESP if your network’s edge firewall is not using NAT-T.

For additional ports and URLs used in a connection between your network and the WSS, see "Reference: Required Locations, Ports, and Protocols" on page 51.

Blueprint Configuration—Configure Certificate Authentication for VPN Connection(s)

The following blueprint demonstrates a command line configuration. To see a user interface reference configuration for a Cisco ASA device, see https://support.symantec.com/en_US/article.TECH254715.html.

Step 1—Obtain the one-time password/authentication token.

The one-time password (OTP) and authentication token are required to obtain and validate authentication certificates used by the VPN device and the WSS.

1. In Service Mode, select Account Maintenance > MDM, API Keys.

2. If you do not already have an account to create WSS APIs, create one.

   a. In Service Mode, select Account Maintenance > MDM, API Keys.

   b. In the API section (bottom half of the screen), click Add API Key.

   c. Define a Username and Password.

      The username must be unique as it used by the WSS to link your account to the location. If the service detects
any other API with the same name, the service displays an error message and you must define another name.

d. Click Add.

3. In the browser, enter the API generation string.

https://cloudwebsecurity.att.com/api/locations?name=location_name&type=cert-firewall

Where location_name is the name you assign. For example:
https://cloudwebsecurity.att.com/api/locations?name=Store103&type=cert-firewall

Creates a new location, Store103, and defines it as a cert-based firewall IPsec connection.

4. The WSS generates the OTP. For example:

{"oneTimePassword":"4d2e183e-1936-4ffc-b298-00ef9529d1d0"}

Record this value to your planning form or somewhere accessible. You need this string value (without the quotes) when configuring your VPN device in Step 3.2 below.

- The OTP remains valid for one week. After that, you must generate a new one.
- If you call a new API but use the same location, you receive a new OTP; however, a 30-day timer begins. At the end of the 30 days, the WSS revokes the previous certificate.

5. Verify that the WSS created the new location in Service mode, select Network > Locations.

![Locations](image)

Note: The following recommended details are not specific to any VPN device. If you are not certain of your firewall or VPN appliance’s supported capabilities, options, or configuration steps, consult AT&T support, as they might be able to advise the best configuration or help you work with your VPN device vendor’s support team for assistance.
Step 2—Import the root certificate (Entrust 2048-bit) to your VPN device.

AT&T partners with Entrust to provide authentication certificates. You must import the 2048-bit certificate to your VPN device. Because of the complexity of this process, command steps to configure a Cisco IOS device are provided in the following example. Consult your VPN device documentation to determine the analogous steps for your device.

1. In a browser, navigate to–

   https://www.entrust.com/get-support/ssl-certificate-support/root-certificate-downloads/

   a. Locate the Root Certificate identified by the following:

   - **Serial Number**: 45 6b 50 54
   - **Thumbprint**: b3 1e b1 b7 40 e3 84 02 da dc 37 d4 4d f5 d4 67 49 52 f9

   b. Click Download and open the file in a text editor.

2. Access the VPN device CLI.

3. Create a trustpoint for the CA root certificate.

   ```
   device#configure terminal
   device(config)#crypto pki trustpoint entrust2006
   device(ca-trustpoint)#enrollment terminal PEM
   device(ca-trustpoint)#crl optional
   device(ca-trustpoint)#exit
   ```

4. Import (copy and paste) the root certificate.

   ```
   device(config)#crypto ca authenticate entrust2006
   Enter the base 64 encoded CA certificate.
   End with a blank line or the word "quit" on a line by itself
   -----BEGIN CERTIFICATE-----
   MIIEjCCAXkgAwIBAgIEOGPe+DANBgkqhkiG9w0BAQUFADCBtDEUMBIGA1UEChM7
   <snip>
   -----END CERTIFICATE-----
   quit
   Certificate has the following attributes:
   Fingerprint MD5: D6A5C3ED 5DDD3E00 C13D8792 1F1D3FE4
   Fingerprint SHA1: B31EB1B7 40E36C84 02DADC37 D44DF5D4 674952F9
   % Do you accept this certificate? [yes/no]: yes
   Trustpoint CA certificate accepted.
   % Certificate successfully imported
   ```

5. Verify that the certificate successfully imported.

   ```
   device#show crypto pki certificates entrust2006
   CA Certificate
   Status: Available
   ```
Certificate Serial Number (hex): value
Certificate Usage: Signature
Issuer:
  cn=Entrust Root Certification Authority
  ou=(c) 2006 Entrust Inc.
  ou=www.entrust.net/CPS is incorporated by reference
  o=Entrust, Inc.
  c=US
Subject:
  cn=Entrust Root Certification Authority
  ou=(c) 2006 Entrust Inc.
  ou=www.entrust.net/CPS is incorporated by reference
  o=Entrust, Inc.
  c=US
Validity Date:
  start date: 20:23:42 UTC Nov 27 2006
  end date: 20:53:42 UTC Nov 27 2026
Associated Trustpoints: entrust2006-2 entrust2006 <<--matches the trustpoint configured in Step 1.3-->>.
Storage: nvram:EntrustRootC#5050CA.cer

Step 3—Configure your VPN device to perform a SCEP request to enroll the device.

1. If the device does not already have a key-pair, you must generate one.

```
device(config)#crypto key generate rsa modulus 2048 label
```

2. Create a trustpoint for the certificate from the SCEP service (Entrust). IMPORTANT: The trustpoint name must be BlueCoatIssuingCA.

   This step requires your OTP that you obtained in Step 1 and the label name. Do not enter the quotation marks—just the value within.

```
device(config)#crypto pki trustpoint BlueCoatIssuingCA
device(ca-trustpoint)#enrollment url http://bluecoatasweb.managed.entrust.com/scep
device(ca-trustpoint)#password one_time_password
device(ca-trustpoint)#rsakeypair label
device(ca-trustpoint)#exit
```

3. Authenticate and enroll the trustpoint.

```
device(config)#crypto pki authenticate BlueCoatIssuingCA
device(config)#crypto pki enroll BlueCoatIssuingCA
```

4. Verify the successful certificate download.
Step 4—Establish the authenticated VPN device-to-WSS tunnel.

In the final step, configure your VPN device to communicate with the WSS, which authenticates the device authentication certificate, and route web-destination traffic to the cloud service. Again, we use a Cisco 891 for this example. Refer to your VPN device vendor's documentation for specific instructions for your device.

1. Define the Internet Security Association and Key Management Protocol (ISAKMP), which establishes Security Associations (SA) and cryptographic keys (RFC 2408).

```
device#crypto isakmp identity dn
device#crypto isakmp keepalive 10 periodic
device#crypto isakmp nat keepalive 60
device#crypto isakmp aggressive-mode disable
```

2. Create a certificate map match to the certificate sent by the AT&T service. The following example (and subsequent example commands) use bccs as the map name. The certificate on the WSS maps the name to *.threatpulse.com.

```
device#crypto pki certificate map bccs 1
name co threatpulse
!
```

3. Create the ISAKMP profile used for the WSS connection. (the name BlueCoat is used only as an example)

```
device#crypto isakmp profile bccs
ca trust-point entrust2006
crs trust-point BlueCoatIssuingCA
match certificate bccs
!
```


```
device#crypto ipsec transform-set ESP-AES-256-MD5 esp-aes esp-md5-hmac
```

5. Configure the IPsec connection. Refer to your planning form for the WSS IP address that you are assigning to this location. In this example and subsequent examples, the crypto map is named BCCS_CMAP_1. Refer to your planning sheet.

```
device#crypto map BCCS_CMAP_1 1 ipsec-isakmp
set peer threatpulse_service_vip
set transform-set ESP-AES-256-SHA
set pfs group5
set isakmp-profile BlueCoat
match address IPSEC_TRAFFIC
!
```
6. Configure the WAN interface to reference the BCCS_CMAP_1 Crypto Map.

   ```
   device#interface GigabitEthernet0
   crypto map BCCS_CMAP_1
   ```

7. Define web-destination traffic and NAT rules.

   ```
   device#ip nat inside source list nat_rule interface GigabitEthernet0 overload
   !
   device#ip access-list extended IPSEC_TRAFFIC
   permit tcp inside_ip_interface subnet any eq www
   permit tcp inside_ip_interface subnet any eq 443
   device#ip access-list extended nat_rule
   deny tcp inside_ip_interface subnet any eq www
   deny tcp inside_ip_interface subnet any eq 443
   permit ip inside_ip_interface subnet any
   ```

**Step 5—Ensure Dead Peer Detection is enabled.**

Dead Peer Detection (DPD)— Depending on your VPN device and network configuration, AT&T recommends that DPD is set to check every thirty seconds with five retries.

The following is known list of common vendor instructions for DPD:

- Cisco Router info for DPD- [Cisco Routers DPD](#)
- Cisco Community DPD Article- [Cisco DPD Info](#)
- Checkpoint DPD Info - [Checkpoint KB on DPD](#)
- Juniper DPD - [Juniper DPD Info](#)
- Palo Alto DPD - [Palo Alto DPD KB](#)
- Fortinet Fortigate DPD - [Fortigate DPD](#)
- If your manufacturer is not listed, consult their website or support team for assistance with this feature.

**Helpful Tips**

The following knowledge base articles cover the most common issues faced by network administrators working with VPN tunnels and their remedies.

- Data Center Egress IP Addresses. The following articles list the public IP addresses used to reach Internet resources from Cloud Web Security Service service worldwide:

- Browser Error on IPsec VPN if First Request is HTTPS: https://support.symantec.com/en_US/article.TECH246221.html

Next Selection

- IPsec deployment: Proceed to "Verify Connections" on page 43.
- Explicit Over IPsec deployment: Add the explicit proxy entry to PAC file. See "Connectivity: Explicit Over IPsec" on the next page.
Connectivity: Explicit Over IPsec

An Explicit Over IPsec deployment is one where the same web request is instigated by the browser as an explicit proxy connection but is sent to the Cloud Web Security Service over an IPSec tunnel. This is a type of deployment that can be used with any of the IPSec location types supported by WSS. This method is most commonly used in environments where a default route to the internet does not exist, such as an environment with tighter control, where browsers only have one controlled/explicit way out via a PAC file.

Technical Requirements

This section provides a high-level set of technical requirements required to perform this configuration.

- Your organization has been provisioned with an account in the WSS.
  
  To confirm this, browse to https://portal.threatpulse.com and log in. If you are unable to log in, verify your account details with AT&T support.

- An understanding of how much user traffic will route to the Cloud Web Security Service.
  
  The WSS is limited to 500mbit/s of bandwidth per IPSec tunnel. If you expect traffic to exceed that, you must plan your architecture to use an additional tunnel from an additional public IP address for each 500mbit/s block of bandwidth you expect to consume. For example, if one of your sites consumes 900mbit/s of traffic, it must connect to the WSS using at least two IPSec tunnels, each connecting from a unique public IP address.

- The internal network addresses that is the source of data to send to the WSS.

  For example, as a best practice do not send intranet resources, such as email and internal web services, through the tunnel. Additionally, exclude the server where the Auth Connector is installed from the tunnel as it makes a direct connection to the WSS through port 443. See "Forward Specific User and Group Names to the Service" on page 41.

- If your proxy forwarding deployment handles traffic for a large number of users, you must configure your ProxySG appliance to use more source ports than the 1024 used by default, and to segregate that traffic to ensure appropriate balancing of your connection load to the service. Follow the steps in this KB article https://support.symantec.com/en-US/article.TECH254332.html.

Procedure

Step 1—Configure a VPN Connection to the WSS

Configure the gateway VPN device to route internet-bound traffic to the WSS.

- "Connectivity: VPN Pre-Shared Key with Static IP" on page 12
- "Connectivity: VPN IKEv2 with Pre-Shared Key and Dynamic IP/FQDN" on page 19
- "Connectivity: VPN Certificate Authentication" on page 30

If you are unsure of which method is required for your network environment, see "Connectivity—About Virtual Private Network (IPsec)" on page 5.
Step 2—Configure Client Browsers to Explicit Proxy to the VPN Device

To configure explicit over IPsec solution, you must add an entry to your PAC file. This entry instructs all outbound web traffic to use a proxy and the route to this proxy will be through an IPsec tunnel to the WSS.

The following three scenarios support this:

- All clients require the explicit proxy connection to the web. For example, in a no default gateway route topology or one that employs an Interior Gateway Protocol (IGP). The entry for this method is:

  ```
  return "PROXY ep.threatpulse.net:80";
  ```

- You have an on-premise proxy securing your web traffic and want to use the WSS as a backup proxy option. You ensure that traffic sent to proxy.threatpulse.net:8080 uses the VPN tunnel to the WSS. The entry for this method is:

  ```
  return "PROXY corp-gw.mycompany.com:8080; PROXY ep.threatpulse.net:8080";
  ```

- You have configured an on-premise proxy to secure web traffic, but want to use an explicit over IPsec connection method to provide seamless back up to that. In this instance, your site’s edge firewall only permits traffic out to the Internet on port 80, while your proxy is configured to listen for requests on port 8080. You ensure that traffic sent to proxy.threatpulse.net:80 uses the VPN tunnel to the WSS. The entry for this method is:

  ```
  return "PROXY corp-gw.mycompany.com:8080; PROXY ep.threatpulse.net:80";
  ```

Example PAC File

The following example provides typical enterprise PAC file contents. The Explicit over IPsec entry is at the end.

```javascript
function FindProxyForURL(url, host)
{
    /* SPECIAL CASES FOR NON-BALANCED ROUTING */
    // Direct connections to non-FQDN hosts
    if (isPlainHostName(host) ||
        (host == "127.0.0.1") ||
        (host == "www.symantec.example.com") ||
        (host == "symantec.example.com") ||
        (shExpMatch(host, "*.symantec-intranet.com")) ||
        (shExpMatch(host, "90.0.0.*")) ||
        (shExpMatch(host, "10.*"))) {
        return "DIRECT"
    } else {
        return "PROXY ep.threatpulse.net:8080"
    }
}
```

Common Troubleshooting Tips

The following knowledge base articles cover the most common issues faced by network administrators working with VPN tunnels and their remedies.

- Data to collect before opening a support case with AT&T support: https://support.symantec.com/en_US/search.html?product=&keyword=TECH203533
Data Center Egress IP Addresses. The following articles list the public IP addresses used to reach Internet resources from the Cloud Web Security Service service worldwide:


Enable SSL Interception in the WSS: https://support.symantec.com/en_US/article.TECH241098.html

Browser Error on IPsec VPN if First Request is HTTPS: https://support.symantec.com/en_US/article.TECH246221.html
Forward Specific User and Group Names to the Service

By default, the Auth Connector returns all group and usernames that are contained in your LDAP deployment to the AT&T Cloud Web Security Service for use in custom policy creation. This might not be practical for an enterprise network that contains multiple user groups and large volumes of users. Sending that much information might cause Auth Connector resource constraints. AT&T recommends performing this before installing the Auth Connector.

For large LDAP deployments, AT&T recommends selecting all users, but decide which groups require policy and forward only those to the Cloud Web Security Service. For example, you have domains named HQ-QA, HQ-SALES, and HQ-OPERATIONS and only users in the HQ-SALES domain require policy checks.

The `bcca.ini` file, which is part of the Auth Connector application, contains `[Groups]` and `[Users]` sections. You can add entries to one, either, or both:

- If the `[Groups]` and `[Users]` sections are empty, the WSS receives traffic from all domains and users.
- If the `[Groups]` section contains a domain entry (for example, HQ-SALES\), then all groups within that domain send traffic to the cloud service.
- To further narrow the scope with domains, add group names. For example: HQ-SALES\RegionA.
- The `[Users]` section functions in the same manner. Add specific users to even further limit whose traffic is sent to the cloud services. For example: HQ-SALES\thomas.hardy.

**Note:** To prevent a full transmission of all user and group names, do not open the firewall for outbound 443/tcp from the Auth Connector before you complete this task.

### Procedure

This process to add domains, users, and groups is manual.

1. Access the server that has the Auth Connector application.
2. Using a text editor, open the `bcca.ini` file. If you installed the Auth Connector in the default directory, find it in: `C:\Program Files\Blue Coat Systems\BCCA`.
3. Locate the `[Groups]` and `[Users]` sections and add entries. You must use the same letter cases that match what is in the Active Directory. Add one entry per line. For example:

   ```ini
   [Groups]
   HQ-SALES\NAWest
   HQ-SALES\NANorthWest
   [Users]
   HQ-SALES\Administrator
   ```
4. Save the file.
5. Allow the service to process some traffic, then check various reports to verify that you are receiving traffic from the specified groups/users.
Verify Connections

After configuring access to the AT&T Cloud Web Security Service, verify that the service is receiving and processing content requests.

Verify Client Protection

From a client system that has web access (or the specific test client if so configured), browse to the following site:

test.threatpulse.com

The test is successful if you see the following webpage.

Fixed Locations

1. Click the Service link (upper-right corner).
2. Select Network > Locations.
3. Verify the status of each location.
Various icons represent the connection status.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Connection Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Check" /></td>
<td>The Cloud Web Security Service recognizes the location and accepts web traffic.</td>
</tr>
<tr>
<td><img src="image" alt="Orange Exclamation" /></td>
<td>A location has been configured, but the Cloud Web Security Service cannot connect. Verify that the web gateway device is properly configured to route traffic.</td>
</tr>
<tr>
<td><img src="image" alt="Bell" /></td>
<td>A previously successful web gateway to Cloud Web Security Service configuration is currently not connected.</td>
</tr>
</tbody>
</table>

- **Firewall/VPN**
  - Verify your firewall’s public gateway address.
  - Verify the Preshared Key (PSK) in the portal matches that of your firewall configuration.
  - Verify that the server authentication mode is set to PSK.
- **Explicit Proxy**
  - Verify the PAC file installation and deployment.
  - Verify that your network allows outbound requests on port 8080.
  - Do not attempt to use Explicit Proxy in conjunction with the WSS Agent as the client will detect that a proxy is in effect, assume a man-in-the-middle attack, and fail (open or closed depending on the settings).
- **Proxy Forwarding**—Verify the gateway address in the forwarding host is correct.
- **Remote Users**—Verify the WSS Agent installation. See the section below for more information.

**Remote Users**

In **Service Mode**; select **Mobility > Agent Status**.
To further verify that the agent in running on remote clients and communicating with the WSS:

- For WSS Agent, see the WSS Agent topics.
- For Unified Agent, click (or double-click) the application icon in the menu bar and click **Status**.

### Windows (UA)

If the system detects a corporate network that provides web access and security, the Unified Agent enters into passive mode.
Mac (UA)

If the system detects a corporate network that provides web access and security, the Unified Agent enters into passive mode.
Reference

This section provides information required for proper firewall device and network configurations.

- "Reference: Cloud Web Security Service Data Center Ingress IPs" on page 49
- "Reference: Egress IP Ranges" on page 50
- "Reference: Required Locations, Ports, and Protocols" on page 51
- "Reference: IKE Encryption and Authentication Algorithms" on page 54
Reference: Cloud Web Security Service Data Center Ingress IPs

Fixed-location Access Methods require you to enter IP addresses of the nearest Cloud Web Security Service datacenter(s).

You also must add these IP addresses plus the Cloud Web Security Service portal to your firewall's allowed outbound rules.

The Symantec Operations team maintains the following Knowledge Base article.

Reference: Egress IP Ranges

Protected traffic is tunneled through the AT&T Cloud Web Security Service. You might require this information because the egress IP address is no longer the IP address of your network.

The Symantec Operations team maintains the following region-based Knowledge Base articles. These articles include Web Isolation addressees.

### Reference: Required Locations, Ports, and Protocols

Depending on your configured AT&T Cloud Web Security Service Access Methods, some ports, protocols, and locations must be opened on your firewalls to allow connectivity to the various cloud service components and data centers.

### Symantec Resource

**support.symantec.com**

Support site links to support tools and documentation.

### Access Methods

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Resolves To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Web Security Service Portal Access</td>
<td>443</td>
<td></td>
<td>cloudwebsecurity.att.com</td>
</tr>
<tr>
<td>For administration of your WSS policy and configuration.</td>
<td></td>
<td></td>
<td>199.19.250.192</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.116.168.192</td>
</tr>
<tr>
<td>Firewall/VPN (IPsec)</td>
<td>UDP 500 (ISAKMP)</td>
<td>IPsec/ESP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP4500 if firewall is behind a NAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy Forwarding</td>
<td>TCP 8080/8443</td>
<td>HTTP/HTTPS</td>
<td>proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td>TCP 8084*</td>
<td></td>
<td>If this forwarding host is configured for local SSL interception.</td>
</tr>
</tbody>
</table>
| Explicit Proxy                                     | TCP 443 |          | • Firewall rules to allow PFMS access:
| SEP PAC File Management System or Default PAC file |         |          | ◦ By hostname: pfms.wss.symantec.com             |
|                                                    |         |          | ◦ By IP Address:                                 |
|                                                    |         |          | ○ 35.155.165.94                                 |
|                                                    |         |          | ○ 35.162.233.131                                |
|                                                    |         |          | ○ 52.21.20.251                                  |
|                                                    |         |          | ○ 52.54.167.220                                 |
|                                                    |         |          | ○ 199.247.42.187                                |
|                                                    |         |          | ○ 199.19.250.187                                |
| Default PAC file: TCP 8080                         |         |          | • The default PAC file directs browser traffic to proxy.threatpulse.net. |
### Access Method

**Explicit Over IPsec (Trans-Proxy)**

In this deployment method, all traffic is transmitted from your network to WSS. Two scenarios are common.

- **On-premises ProxySG appliance.**
  
  Explicit browser settings direct traffic to the proxy, which forwards that traffic to the WSS through a configured IPsec tunnel.

- **Explicit settings in the browser pointed to ep.threatpulse.net.**
  
  Direct all firewall traffic destined for ep.threatpulse.net to WSS through your configured IPsec tunnel.

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Resolves To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit Over IPsec (Trans-Proxy)</td>
<td>UDP 500 (ISAKMP)</td>
<td></td>
<td>ep.threatpulse.net resolves to 199.19.250.205</td>
</tr>
<tr>
<td></td>
<td>UDP4500 if firewall is behind a NAT.</td>
<td></td>
<td>ep-all.threatpulse.net returns the following.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.248.205</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.205</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.206</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.207</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.208</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.209</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.210</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.211</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.212</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.213</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.214</td>
</tr>
<tr>
<td></td>
<td>ep-roundrobin.threatpulse.net returns all IPs in a round-robin fashion; each two-minute Time-To-Live (TTL) period returns a different address.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WSS Agent</td>
<td>TCP/UDP 443</td>
<td>SSL</td>
<td>ctc.threatpulse.com (for TCP, UDP, and software updates)</td>
</tr>
<tr>
<td>Unified Agent</td>
<td>TCP 80</td>
<td>TCP, SSL</td>
<td>Port 80/443 to portal.threatpulse.com (199.19.250.192) (for captive network information and updates)</td>
</tr>
<tr>
<td></td>
<td>TCP/UDP 443</td>
<td></td>
<td>Port 443 to ctc.threatpulse.com Port 443 to client.threatpulse.net (DNS fallback)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TCP port 443 to client.threatpulse.net (DNS fallback), UDP added for agent version v4.9.1 or above.</td>
</tr>
<tr>
<td>Mobile (SEP-Mobile iOS/Android app)</td>
<td>UDP 500 (ISAKMP)</td>
<td>IPSec/ESP</td>
<td>199.19.250.195</td>
</tr>
<tr>
<td></td>
<td>UDP 4500 (NAT-T)</td>
<td></td>
<td>199.116.168.195</td>
</tr>
<tr>
<td>Hybrid Policy</td>
<td></td>
<td></td>
<td>If connectivity to the WSS is behind stringent firewall rules, adjust the rules to allow traffic to pass to these IP addresses on port 443.</td>
</tr>
</tbody>
</table>
### Authentication

<table>
<thead>
<tr>
<th>Auth Method</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Resolves To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Connector</td>
<td>TCP 443</td>
<td>SSL</td>
<td>to auth.threatpulse.com:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.193</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.116.168.193</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cloudwebsecurity.att.com:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.192</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Tip:</strong> Additional Required Information: &quot;Reference: Authentication IP Addresses&quot; on page 58.</td>
</tr>
<tr>
<td>Auth Connector to Active Directory</td>
<td>TCP 139,445</td>
<td>SMB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 389</td>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 3268</td>
<td>ADSI LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 135</td>
<td>Location Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 88</td>
<td>Kerberos</td>
<td></td>
</tr>
<tr>
<td></td>
<td>49152-65535</td>
<td>TCP</td>
<td>If installed on a new Windows Server 2012 Member rather than a Domain Controller.</td>
</tr>
<tr>
<td>AC-Logon App</td>
<td>TCP 80</td>
<td></td>
<td>Port 80 from all clients to the server.</td>
</tr>
<tr>
<td>SAML</td>
<td>TCP 8443 (over VPN)</td>
<td>Explicit and IPSec</td>
<td>to saml.threatpulse.net</td>
</tr>
<tr>
<td>Roaming Captive Portal</td>
<td>TCP 8080</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cloud-to-Premises DLP

For connection coordination and management status.

- Port 443 (traffic from client device)
- XMPP port 5222 to comm.threatpulse.com
Reference: IKE Encryption and Authentication Algorithms

Configuring a router device for the AT&T Cloud Web Security Service Firewall/VPN Access Method requires selecting Internet Key Exchange algorithms, which are used to create a channel over which IPsec Proposals negotiate and encrypt HTTP traffic.

The Cloud Web Security Service supports the following combinations, with following caveat.

Note: AT&T did not test every combination. Although the expectation is these are supported, AT&T recommends performing your own verification.

Encryption Algorithms

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes128</td>
<td>128 bit AES-CBC</td>
<td>aes192</td>
<td>192 bit AES-CBC</td>
</tr>
<tr>
<td>aes256</td>
<td>256 bit AES-CBC</td>
<td>aes128ctr</td>
<td>128 bit AES-COUNTER</td>
</tr>
<tr>
<td>aes192ctr</td>
<td>192 bit AES-COUNTER</td>
<td>aes256ctr</td>
<td>256 bit AES-COUNTER</td>
</tr>
<tr>
<td>aes128ccm8</td>
<td>128 bit AES-CCM with 64 bit ICV</td>
<td>aes192ccm8</td>
<td>192 bit AES-CCM with 64 bit ICV</td>
</tr>
<tr>
<td>aes256ccm8</td>
<td>256 bit AES-CCM with 64 bit ICV</td>
<td>aes128ccm12</td>
<td>128 bit AES-CCM with 96 bit ICV</td>
</tr>
<tr>
<td>aes192ccm12</td>
<td>192 bit AES-CCM with 96 bit ICV</td>
<td>aes256ccm12</td>
<td>256 bit AES-CCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes128ccm16</td>
<td>128 bit AES-CCM with 128 bit ICV</td>
<td>aes192ccm16</td>
<td>192 bit AES-CCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes256ccm16</td>
<td>256 bit AES-CCM with 128 bit ICV</td>
<td>aes128gcm8</td>
<td>128 bit AES-GCM with 64 bit ICV</td>
</tr>
<tr>
<td>aes192gcm8</td>
<td>192 bit AES-GCM with 64 bit ICV</td>
<td>aes256gcm8</td>
<td>256 bit AES-GCM with 64 bit ICV</td>
</tr>
<tr>
<td>aes128gcm12</td>
<td>128 bit AES-GCM with 96 bit ICV</td>
<td>aes192gcm12</td>
<td>192 bit AES-GCM with 96 bit ICV</td>
</tr>
<tr>
<td>aes256gcm12</td>
<td>256 bit AES-GCM with 96 bit ICV</td>
<td>aes128gcm16</td>
<td>128 bit AES-GCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes192gcm16</td>
<td>192 bit AES-GCM with 128 bit ICV</td>
<td>aes256gcm16</td>
<td>256 bit AES-GCM with 128 bit ICV</td>
</tr>
<tr>
<td>aes128gmac</td>
<td>Null encryption with 128 bit AES-GMAC</td>
<td>aes192gmac</td>
<td>Null encryption with 192 bit AES-GMAC</td>
</tr>
<tr>
<td>aes256gmac</td>
<td>Null encryption with 256 bit AES-GMAC</td>
<td>3des</td>
<td>168 bit 3DES-EDE-CBC</td>
</tr>
<tr>
<td>blowfish128</td>
<td>128 bit Blowfish-CBC</td>
<td>blowfish192</td>
<td>192 bit Blowfish-CBC</td>
</tr>
<tr>
<td>blowfish256</td>
<td>256 bit Blowfish-CBC</td>
<td>camellia128</td>
<td>128 bit Camellia-CBC</td>
</tr>
<tr>
<td>camellia192</td>
<td>192 bit Camellia-CBC</td>
<td>camellia256</td>
<td>256 bit Camellia-CBC</td>
</tr>
</tbody>
</table>
**Integrity Algorithms**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>MD5 HMAC</td>
<td>96 bit</td>
</tr>
<tr>
<td>sha1 or sha</td>
<td>SHA1 HMAC</td>
<td>96 bit</td>
</tr>
<tr>
<td>sha256 or sha2_256</td>
<td>SHA2_256_128 HMAC</td>
<td>128 bit</td>
</tr>
<tr>
<td>sha384 or sha2_384</td>
<td>SHA2_384_192 HMAC</td>
<td>192 bit</td>
</tr>
<tr>
<td>sha512 or sha2_512</td>
<td>SHA2_512_256 HMAC</td>
<td>256 bit</td>
</tr>
<tr>
<td>aesxcbc</td>
<td>AES XCBC</td>
<td>96 bit</td>
</tr>
<tr>
<td>aes128gmac</td>
<td>128-bit AES-GMAC</td>
<td>128 bit</td>
</tr>
<tr>
<td>aes192gmac</td>
<td>192-bit AES-GMAC</td>
<td>192 bit</td>
</tr>
<tr>
<td>aes256gmac</td>
<td>256-bit AES-GMAC</td>
<td>256 bit</td>
</tr>
</tbody>
</table>

**Diffie-Hellman Groups**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>DH Group</th>
<th>Modulus</th>
</tr>
</thead>
<tbody>
<tr>
<td>modp1024</td>
<td>2</td>
<td>1024 bits</td>
</tr>
<tr>
<td>modp1536</td>
<td>5</td>
<td>1536 bits</td>
</tr>
<tr>
<td>modp2048</td>
<td>14</td>
<td>2048 bits</td>
</tr>
<tr>
<td>modp3072</td>
<td>15</td>
<td>3072 bits</td>
</tr>
<tr>
<td>modp4096</td>
<td>16</td>
<td>4096 bits</td>
</tr>
<tr>
<td>modp6144</td>
<td>17</td>
<td>6144 bits</td>
</tr>
<tr>
<td>modp8192</td>
<td>18</td>
<td>8192 bits</td>
</tr>
</tbody>
</table>

**Modulo Prime Groups with Prime Order Subgroup**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>DH Group</th>
<th>Modulus</th>
</tr>
</thead>
<tbody>
<tr>
<td>modp1024s160</td>
<td>22</td>
<td>1024 bits</td>
</tr>
<tr>
<td>modp2048s224</td>
<td>23</td>
<td>2048 bits</td>
</tr>
<tr>
<td>modp2048s256</td>
<td>24</td>
<td>2048 bits</td>
</tr>
</tbody>
</table>

**Cisco ASA Devices**

The Cisco ASA device-to-Cloud Web Security Service access method requires selecting a supported **IPsec Proposal**. Cisco references groups of these as *transform sets*. If the device does not already have supported encryption/authentication protocols configured, you must create them. AT&T uses and recommends Cipher Block Chaining (CBC) mode.

1. Select **Configuration**.
2. Click **Site-to-Site VPN**.
3. Click **Add**. The device displays the Add IPsec Site-to-Site Connection Profile.
4. In the Encryption Algorithms section, click IPsec Proposal: Select. The Select Transforms Set dialog displays. Review the list, looking for currently supported proposals. Create a new one, if required.

   a. Click Add. The Add Transform Set dialog displays.
   b. Name the proposal; for example, PRE-G5-AES128-SHA.
   c. For the Tunnel option, select Mode.
   d. For the ESP Encryption option, select a supported encryption type (AT&T recommends AES128).
   e. Select an ESP Authentication option (AT&T recommends SHA).
   f. Click OK to close the dialog.

5. In the Assigned IPsec Proposals area, clear all listed proposals and Assign the one you just created.

6. Click OK to close this dialog.

7. In the IKE Proposals area, verify that the options are 3DES or AES. Click Manage and delete others.

8. Click OK.

9. Return to Select a Firewall Device.

Juniper SSG20 Devices

The Juniper SSG20 device-to-Cloud Web Security Service access method requires selecting a supported Phase 1 (encryption) and Phase 2 (authentication) Proposals protocol. If the device does not already have supported encryption/authentication
protocols configured, you must create them.

**Tip:** If you require more information about Proposals, navigate to the SSG20 page listed in Step 1 and click the Help (?) button.

1. Select **VPNs > AutoKey Advanced > P1 Proposal**.
2. Click **New**. The device displays the **P1 Proposal > Edit** page.
3. Set the encryption options.

![Encryption Options](image)

- **Name** the object. For example, **WSSEncryption**.
- The **Authentication Method** option must be **Preshare**.
- The **DH Group** (Diffie-Hellman) option can be **Group 2** or **Group 5**.
- The **Encryption Algorithm** option can have a **3DES** or **AES (128 or 256 bits)** prefix.
- The **Hash Algorithm** option can be **MD5** or **SHA1**.
- Set the **Lifetime** value. The default value of **28800** seconds is acceptable.
- Click **OK**.

4. Repeat **Steps 2 and 3** for the **AutoKey Advanced > P2 Proposal** page to set the authentication protocol.
5. Return to Select a Firewall Device.
Reference: Authentication IP Addresses

The Cloud Web Security Service Auth Connector communicates with devices in the geographically located data centers.

The Symantec Operations team maintains the following Knowledge Base article.

About the All Ports License

When firewall devices are configured with the standard Firewall/VPN Access Method, the Cloud Web Security Service datapods in the AT&T datacenters listen for web traffic sent only from ports 80 and 443. The Cloud Web Security Service drops traffic from all other ports. Some devices, however, cannot be configured to selectively send only ports 80/443. These devices require the Cloud Web Security Service to pass-through all ports rather than drop traffic from non-web ports.

You cannot achieve this solution through portal configuration. AT&T offers an All Ports License. After you purchase this license and AT&T provisions it, the Cloud Web Security Service portal provides verification that the service is implementing this functionality.

Select Service mode > Network > Locations. The portal displays an All Ports status.

All ports are being accepted by the Cloud Web Security Service from Firewall/VPN Locations.

About license expiration.

- When the license is within 60 or fewer days from expiration, the Cloud Web Security Service displays a warning message at the bottom of this page.
- If you allow the license to expire, the Cloud Web Security Service returns to dropping non-port 80/443 web traffic and the message at the bottom of the page indicates this status.

If you require this functionality, contact your AT&T sales representative.
Solve a Problem

The following tasks might assist you with Firewall/VPN connection issues.

- "Troubleshoot IPsec/VPN/Firewall Connections" on the next page
- "Stop Sending Traffic from a Location" on page 63
Troubleshoot IPsec/VPN/Firewall Connections

If you are having problems with IPsec/VPN/Firewall connections to the AT&T Cloud Web Security Service, refer to the following action steps.

**Verify that the IPsec tunnel is established.**

On the remote peer, use one of the following commands:

- Cisco ASA—# show ipsec sa
- Juniper SSG20—> get sa

**Verify that the peer IP address for your tunnel is correct.**

It must be a valid Cloud Web Security Service IP address. Plan the Firewall Device Configuration

**Verify that peer IP address is reachable from the router.**

Can you ping the Cloud Web Security Service IP address from the router?

**Verify that the Preshare Key (PSK) is correct.**

Verify that you entered the same PSK in router and in Cloud Web Security Service interface.

For failover, the PSK must be configured for all peers.

**Dead Peer Connections must be enabled.**

Verify that the Dead Peer Connection option is enabled.

**Use supported proposal/transform sets**


**Create correct tunnel definitions on your gateway.**

The Cloud Web Security Service supports only two types of Phase 2 proposals:

- <any internal (RFC 1918) subnet>:6/0 <--- 0.0.0.0:6/80
- <any internal (RFC 1918) subnet>:6/0 <--- 0.0.0.0:6/443

For example, TCP from internal address—any port to any address port 80 or port 443.

**Verify correct NAT rules for all non-Cloud Web Security Service-destined traffic.**

- TCP port 80 and port 443 traffic.
- NAT Auth Connector traffic destined on port 443.
- Include any other IP traffic (such as UDP, ICMP)
Juniper KB Article Link.

- http://kb.juniper.net/InfoCenter/index?page=content&id=KB9221
Stop Sending Traffic from a Location

Currently, there is not a one-click option in the AT&T Cloud Web Security Service interface to temporarily stop or bypass traffic from a special location (with exception of individual remote user clients; see below). The following are possible workarounds:

Delete Location

1. In Service Mode, select Network > Locations.
2. Select a location, and click Delete Selection.

To restore the location, you must re-add it.

Connectivity Method

Alter the connectivity method (IPsec, Proxy Forwarding, Explicit Proxy) at the physical location.