The Symantec Web Security Service solutions provide real-time protection against web-borne threats. As a cloud-based product, the Web Security Service leverages Symantec’s proven security technology as well as the WebPulse™ cloud community of over 75 million users.

With extensive web application controls and detailed reporting features, IT administrators can use the Web Security Service to create and enforce granular policies that are instantly 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 Web Security Service for security scanning and policy checks.

- "Learn..." on page 9
- "Reference" on page 22
- "Select a Firewall Device (PSK)" on page 35
- "Select a Firewall Device (Cert-Based)" on page 96
- "Verify Service Connectivity to Locations" on page 171
- "Forward Specific User and Group Names to the Service" on page 175
- "Troubleshoot IPsec/VPN/Firewall Connections" on page 177
- "Stop Sending Traffic from a Location" on page 178
- "Captive Portal Diagnostic Messages" on page 179

This document contains topics collected from the Web Security Service online documentation. For the complete doc set, see:

Symantec Support Site > WSS Documentation

Table Of Contents

Copyrights ......................................................................................................................................... 3

Web Security Service: Firewall/VPN Access Method ........................................................................ 4
    Table Of Contents ........................................................................................................................ 4

Learn... ........................................................................................................................................... 9
    About the Firewall/VPN Access Method .................................................................................. 10
    About Certificate-Based Firewall Connections ....................................................................... 12
    About Challenge-based Auth (Captive Portal) ....................................................................... 14
        Enable Captive Portal? ........................................................................................................ 17
    About Roaming Captive Portal ................................................................................................. 18
        Additional Notes ................................................................................................................ 19
    Implement This Feature? .......................................................................................................... 19
About Trans-Proxy (Explicit Proxy Over IPsec) ................................................................. 20

Topography 1—No Default Route .................................................................................. 20

Topography 2—One Common Proxy Setting ................................................................. 21

Why Select This Method? ............................................................................................... 21

Reference ......................................................................................................................... 22

Plan the Device Configuration ....................................................................................... 23

Step 1—Select Your Deployed Device ............................................................................ 23

Firewall/VPN Access Method ......................................................................................... 23

Certificate-Based Firewall Access Method ....................................................................... 23

Step 2—Select a Regional Web Security Service IP Address ......................................... 23

Step 3—Enter Network Information .............................................................................. 24

Step 4—(Optional) Specify Groups of Interest ............................................................... 24

Reference: Authentication IP Addresses ........................................................................ 26

Reference: IKE Encryption and Authentication Algorithms ........................................... 27

Modulo Prime Groups with Prime Order Subgroup ....................................................... 28

Reference: Required Locations, Ports, and Protocols .................................................... 31

Symantec Resource ......................................................................................................... 31

Access Methods ............................................................................................................. 31

Authentication .................................................................................................................. 32

Cloud-to-Premises DLP ................................................................................................. 33

Reference: Egress IP Ranges .......................................................................................... 34

Select a Firewall Device (PSK) ....................................................................................... 35

Pre-Deployment: Select Authentication Method ............................................................. 35

Pre-Shared Key/Standard Configuration ......................................................................... 35

Check Point Site-to-Site VPN Configuration (PSK) ......................................................... 36

Deployment Notes .......................................................................................................... 36

Procedure ......................................................................................................................... 36

Next Selection .................................................................................................................. 49

Cisco ASA Site-to-Site VPN Configuration (PSK) ........................................................... 50

Deployment Notes .......................................................................................................... 50

Procedure ......................................................................................................................... 50

Next Selection .................................................................................................................. 58

Cisco Meraki Firewall: Create a Site-to-Site VPN ........................................................... 59
Learn...

This section provides the Firewall/VPN Access Method network footprint. There are two types of this method.

- "About the Firewall/VPN Access Method" on the next page
- "About Certificate-Based Firewall Connections" on page 12
- "About Challenge-based Auth (Captive Portal)" on page 14
- "About Roaming Captive Portal" on page 18
- "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20
**About the Firewall/VPN Access Method**

The Firewall/VPN access method enables you to configure your web gateway firewall or router device to send web traffic from the company internal network to the Symantec Web Security Service. This occurs over an Internet Protocol Security (IPsec) connection.

The most basic concept for this method is:

- Configure the device to route all Internet-bound traffic (port 80 and 443) to the Web Security Service by using a site-to-site VPN from an existing firewall device; and
- Configure the device policy rules to send web-based traffic to the service and ignore everything else.
- This is the preshared-key (PSK) method.

Symantec uses industry standard strong encryption algorithms, including AES-256, to ensure all traffic is kept private as it passes to the Web Security Service. During configuration, you specify a pre-shared key for the site-to-site VPN connection. 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.

---

**Data Flow**

1—An employee requests web content.

2—VPN-to-VPN policies on the router/firewall device forward web-destined requests to the Web Security Service. A unique `site_ID` number is obtained during the initial configuration of the Web Security Service portal. Also, Symantec provides service IP addresses based on global geographical location.
3—The Web Security Service extracts the original IP address and contacts the AD server that has the Symantec Auth Connector installed, which is required for user reporting and custom policy creation.

4—The Auth Connector connects to the AD. Assuming a successful credential check from the AD, the Auth Connector returns user/groups of interest membership confirmation.

5/6—The Web Security Service performs the Network Address Translation (NAT), resolves content filtering policy checks, connects to content servers, performs malware scanning, and returns content or policy verdict to the requesting client inside the company network.

7—An employee requests non-web content; the Web Security Service is not involved in the process.

Tip: You can also enable captive portal over IPsec authentication for on-premise Wi-Fi connections.

Supported IPsec Modes

The Symantec Web Security Service supports following IPsec modes.

- **IKEV1 Main Mode PSK authentication using IP as peer IKE (ISAKMP) ID**
  
  The device requires a public IP should be on the device (no NAT router fronting the firewall); the device is identified by that unique egress IP only. This known and unique egress IP is per-device and not the users behind the firewall. The device not cannot NAT the IPs before sending over the tunnel. Doing so prevents the Web Security Service from identifying different users.

- **IKEV1 Main Mode Cert authentication using Certificate DN as peer IKE ID**
  
  See "About Certificate-Based Firewall Connections" on the next page.

- **IKEV2 PSK authentication using FQDN as peer IKE ID**
  
  This IKEv2 with FQDN and PSK supports NAT-T.

Why Select This Method?

- Requires no changes to desktops or servers.
- Authentication and redirection are transparent to end users.
- Functions with all agents, not just browsers.
- Supports client IP-based policy.
- Provides fully secured traffic between the site and the Web Security Service.
- Functions with Microsoft Active Directory (AD).
**About Certificate-Based Firewall Connections**

The certificate-based IPsec firewall connection to the Symantec Web Security Service provides an alternative to the VPN-to-VPN Preshared Key method. Before connecting to the service, the firewall performs a Simple Certificate Enrollment Protocol (SCEP) request to the Symantec partner (Entrust) to obtain the certificate used to authenticate itself to the service.

Consider the cert-based IPsec firewall method for the following deployment use cases.

- There are many firewalls behind the NAT firewall, 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.
- Build environments that connect virtualized routers or firewalls to the Web Security Service with no external IP addresses.
- Connect to the Web Security Service with lower-end, open source routers, which might lack VPN-to-VPN capabilities, or non-NATed firewall devices.

**IMPORTANT:** Currently, Symantec has only tested cert-based firewall connections on the Cisco 891 and ASA 9.1 devices. Similar configurations should work on similar devices that supports SCEP, but Symantec cannot guarantee the results.

- Many aggregated businesses, such as tenants in shopping malls, rely on their property infrastructure to be their ISP. Consider the mall deployment.

1—You log in to the Web Security Service and use the API option to generate a one-time password (OTP) and authentication token. The service imprints your device and location-specific information (and retains it for future, location-based policy creation).
2—Import the Entrust public 2048 certificate (obtained from the Entrust website) to your firewall device

3—Perform a SCEP request that includes the OTP. The request goes to Entrust, the Symantec authentication certificate partner, which returns a certificate to your device.

4—Your device, through the ISP, establishes a VPN tunnel to the Web Security Service, which authenticates the device.

5—With your customer information and location verified, the Web Security Service can now perform Web requests and security/policy services. You can write policy against traffic from this specific location.
About Challenge-based Auth (Captive Portal)

By definition, challenge-based authentication displays a credential dialog to users each time they open a web browser. Users must enter their corporate network username and password into the dialog and click Accept before performing web content requests. In this context, this feature is also commonly referred to as Captive Portal.

The Web Security Service provides the Captive Portal for the following deployment methods:

- As an alternative method to check user credentials rather than the method provided by the Unified Agent application that is installed on remote systems.
- Allows an authentication method for BYOD—employees access the network from their personal devices.
- This option also provides user credential checks for Explicit Proxy (PAC file) deployments.
- Required for SAML Authentication integration (Firewall/VPN and Explicit Proxy Access Methods).
- Quickly configure a browser or device for authentication demonstration.

The following diagram illustrates the various Captive Portal solutions based on employee-to-network connection method. All Captive Portal deployments require the Auth Connector application that integrates with your Active Directory to verify user credentials.
A—Firewall/VPN/Guest WiFi Over IPSec

The Web Security Service recognizes a connection from firewall/router device as a fixed location (versus from a roaming user). Using the Authentication Policy Editor, you can specify the surrogate type (IP address or cookie) and authentication refresh intervals on a per-location basis.

With the proliferation of bring your own devices (BYOD), companies must find a way to accommodate employees who use their personal phones and tablets for both work and personal use. One method is to maintain a separate WiFi for BYOD use. The WiFi network might be seen by the Web Security Service as its own location or as one or subnets. With Captive Portal enabled, users must enter their network credentials. Closing and re-opening a browser window within that time does not trigger a new authentication challenge.

Note: DEPLOYMENT NOTE: The following applies to IP surrogates only. For clients behind NAT'ed firewalls, the Symantec recommends using Cookie Surrogates. After a user authenticates from an IP address, all further requests from that IP address are treated as from that user. If the client is behind a NAT or on a multi-user system, the first user's credentials are used. For example, Employee A requests web content and the Web Security Service successfully authenticates him. Employee B then connects, but she is not
sent an authentication challenge. She is seen as Employee A and thus receives all policy designated for Employee A.

B—Explicit Proxy

By default, the Explicit Proxy access method neither provides authentication nor sends user and group information to the Web Security Service for use in reports or custom policy. To make username/group information available, you must enable the Captive Portal option for each location configured in the Web Security Service.

Using the Authentication Policy Editor, you can specify the authentication refresh intervals on a per-location basis.

C—Remote Users (Unified Agent)

The Symantec Web Security Service provides the Captive Portal as an alternative method to check user credentials rather than the method provided natively by the Unified Agent application that is installed on remote systems.

Without Captive Portal enabled, remote users log into the corporate network using their cached credentials. With Captive Portal enabled, the challenge dialog initiates from the client system, which ensures that the correct person logging in is recorded. This allows the system to be accessed by multiple users. Furthermore, the benefit for network administrators is that you have more control of your network access. If a laptop becomes lost or you need to deny a remote employee access, change their status in the Active Directory and that user's access credentials are now denied.

D—Quick Authentication Demonstration (Roaming Captive Portal)

Roaming Captive Portal allows you to quickly connect a non-enrolled device (mobile device or laptop) to the Web Security Service and receive an authentication challenge. For browsers, this allows the enforcement of employee credentials to access web content. For mobile devices, this allows for quick demonstrations of authentication and policy. These browsers/devices are configured to explicitly proxy to the Web Security Service and a user's corporate e-mail addresses are used to validate access.

Additional Information

- Client systems must have third-party cookies enabled.
- Client systems must have the Symantec Web Security Service SSL Root Certificate on their browsers. This is described in the configuration topics.
- If your enterprise comprises multiple domains, users must enter the full domain name rather than just their login name. For example, they must enter alan.user@company.com, not just alan.user.
- If the Auth Connector becomes unavailable, the user receives the following error message: Authentication server error, connecting as unauthenticated user (also, the Web Security Service adds the event to the diagnostic log). The behavior defaults to what happens when Captive Portal is not enabled. That is, the users' access credentials creates a tunnel. For diagnostic analysis, this Advanced dialog entry is unauthenticated (user_name). For other diagnostic entries, see "Captive Portal Diagnostic Messages" on page 179.
- Verify that each user to be authenticated has their e-mail address attribute populated in the AD (User Properties dialog > General > E-mail). For example, EXAMPLECORP\alan.user has an e-mail attribute of alan.user@examplecorp.com. If you are employing Exchange, default policies automatically create this attribute. If you are not employing Exchange and have a large number of users with undefined e-mail attributes in the AD, search online for resources about how to use a script to populate.

About Challenges

When Captive Portal is enabled:
Challenges are based on each browser session. For example, users are challenged when they open Firefox and then can browse (including new tabs). If they then open an Internet Explorer browser, they must enter their credentials in that browser to continue.

Entered passwords, represented as *auth tokens*, are retained in a *credential cache* on the device in the data center that is processing authentication for that client. They are not stored permanently in the cloud. The Authentication Policy Editor allows you to specify surrogate times for the Firewall/VPN Access Method and credential refresh times for both the Firewall/VPN and Explicit Proxy Access Methods.

The following conditions prompt employees to re-enter their credentials.

- When the user attempts to reconnect to the web after those respective time thresholds.
- Other network activity, such as that employee's data getting moved from one data pod to another.

The Auth Connector abides by the lockout settings in the AD. For example, the AD is configured to allow three attempts to log in. If the third attempt fails, the user is locked out for 30 minutes before they can attempt again.

If a lockout configuration exists and the user triggers it or if the user attempts to use an expired password:

- All web-bound transaction intended for the Web Security Service is dropped; all other traffic continues normally.
- If the fault is an Auth Connector problem, the user connects to the Web Security Service as an *unauthenticated user*.

If you render an employee disabled, the Web Security Service requires 15 minutes to complete the transaction; the employee is still able to browse during that time period.

**Enable Captive Portal?**

- Remote Users—Select Service mode > Mobility > Unified Agent. This page contains the Enable Captive Portal option.
About Roaming Captive Portal

The Symantec Web Security Service Roaming Captive Portal feature allows you to accomplish the following.

- Configure a browser for explicit proxy connections to the service, which then enforces user authentication for web sessions.
- Quickly connect a mobile device on the corporate network and demonstrate cloud service authentication and web protection.

Symantec provides a URL or hostname/port, then use corporate domain e-mail addresses and passwords to attempt access web-based content.

Data Flow

1—A Web Security Service Admin (A) in the California corporate office performs the following tasks:

- Verifies that the Auth Connector is configured and functioning with the Active Directory (AD). This is required to validate user e-mail addresses.
- Adds one or more corporate e-mail domains, which are used by the Auth Connector to validate incoming employee connections.
- Enables Roaming Captive Portal, which yields the roaming PAC file URL.

2—These configurations are made available to all Web Security Service data pods locations on the planet.
3—On a laptop connected to the corporate Wi-Fi (B), configure a browser to explicitly proxy to the Web Security Service roaming PAC file. From the laptop, a tester initiates a web request, which routes to the data pod in California.

- The data pod receives the request. For now, the request registers as coming from a nondescript user. The service returns an HTTP 407 Proxy Authentication Required challenge.
- The tester enters his full corporate e-mail address and network password.
- The Auth Connector matches the domain/e-mail; if the match fails, the connection fails. Upon the first successful match, the data pod receives the policy configuration for this type of access method (assuming this is the first connection).

4—Upon successful challenge and data pod registration, the Web Security Service re-requests the web content. Policy checks and malware scanning occur and the employee receives or is denied the content based on those checks.

5—A tester C) in the remote office in London configures the manual proxy setting on her mobile device, which is connected to the corporate Wi-Fi, to route web traffic to the Web Security Service. The London data pod, having received the e-mail domain, roaming captive portal, and policy configurations, initiates an authentication challenge on the device before allowing web-based content.

Additional Notes

Conflict With Coaching Policies

Known Issue: With Roaming Captive Portal enabled, Firefox and Internet Explorer browser return certificate errors (Secure Connection Failed) when a Coaching or possible Password Override policy is triggered. Chrome authenticates, but then also returns an error. Users can reload the page and receive the content.

Twenty-Four Hour Cached Credential Period

User credentials are stored in the Web Security Service credential cache for 24 hours. If you disable Roaming Captive Portal, a user still has access during that time.

App Proxy-Aware Limitations

Many apps (especially on Android devices) are not proxy-aware; therefore, behavior on mobile devices might be erratic and is expected. The features is designed to quickly demonstrate geo-location-based employee awareness by the Web Security Service. Symantec provides a full Mobile Device Service (MDS) for iOS devices.

Implement This Feature?

This is not a stand-alone product. You must complete the initial configuration process and then configure Roaming Captive Portal from the Service mode > Authentication > Auth Connector page.
About Trans-Proxy (Explicit Proxy Over IPsec)

A trans-proxy deployment is one where the same web request is instigated by the browser as an explicit proxy connection but viewed by the Symantec Web Security Service as a transparent request. This is achieved by installed PAC files on browsers that route to the firewall device, which then provides an IPsec connection to the Web Security Service.

Topography 1—No Default Route

- In network topologies where a default route to the internet does not exist (for example, only uses Interior Gateway Protocol (IGP)), add a browser PAC file entry that routes all web requests to the Web Security Service explicit proxy address; for example: ep.threatpulse.net:80.
- PAC files route web requests to a proxy, which in turns connects to the internet. A second entry in the PAC file provides a backup connection to the Web Security Service.

Because this is an explicit connection, HTTPS traffic travels over port 80 from the browser. The firewall device or proxy then establishes a connection over port 443; therefore, both of these ports must be open.

Data Flow (1)—No Default Route

1A: A client performs a web request (port 80). The browser PAC contains an explicit proxy hostname or IP address for the Web Security Service.

1B: Having received the request, the firewall device connects to the Web Security Service over the only route that is allowed out: ep.threatpulse.net:80.
1C: The Web Security Service performs the Network Address Translation (NAT), resolves content filtering policy checks, connects to content servers, performs malware scanning, and returns content or policy verdict to the requesting client inside the company network.

**Data Flow (2)—Web Security Service Backs Up Explicit Proxy Device**

2A: A client performs a web requests (port 80). The gateway proxy is not available.

2B: The connection defaults to the second PAC file entry for ep.threatpulse.net.

2C: Having received the request, the firewall device connects to the Web Security Service over the only route that is allowed out: ep.threatpulse.net:80.

2D: The Web Security Service performs the Network Address Translation (NAT), resolves content filtering policy checks, connects to content servers, performs malware scanning, and returns content or policy verdict to the requesting client inside the company network.

**Topography 2—One Common Proxy Setting**

If Topography 1 is not suitable, such as you need to have one common proxy setting in the PAC file, you can use proxy - threatpulse.net:8080. For this to work as a Trans-Proxy deployment, the firewall must be configured to send traffic to TCP port 8080 over the IPSec tunnel to the Web Security Service. One advantage is that one common URL that works for Explicit, Trans-Proxy, and Roaming Captive Portal (RCP) access methods.

**Why Select This Method?**

- Allows you to maintain tighter control of your firewall—only one IP address is allowed out.
- Unified Solution—When using a ProxySG appliance to upload logs for hosted reporting, you can view unified reports; that is, the reports contain user data regardless of whether the source was the on-premises ProxySG appliance or the backup trans-proxy configuration.
- Provides the Web Security Service with user information despite the originating explicit proxy configuration.
- Authentication and redirection are transparent to end users.
- Functions with all agents, not just browsers.
- Supports client IP-based policy.
- Provides fully secured traffic between the site and the Web Security Service.
- Functions with Microsoft Active Directory (AD).
- Does not require replication using a management tool, such as Symantec Management Center.
This section provides information required for proper firewall device and network configurations.

- "Plan the Device Configuration" on the next page
- "Reference: Authentication IP Addresses" on page 26
- "Reference: IKE Encryption and Authentication Algorithms" on page 27
- "Reference: Required Locations, Ports, and Protocols" on page 31
Plan the Device Configuration

Complete the forms in the following sheet (one per location).

Step 1—Select Your Deployed Device

The devices listed here were officially tested. Similar models might have varying configuration interfaces. You can configure any device that supports site-to-site VPN. The company adds more devices after they are tested by QA. You can also search the Symantec Knowledge Base, which occasionally provides documented, yet not-as-yet sanctioned device configuration steps.

Firewall/VPN Access Method

<table>
<thead>
<tr>
<th>Vendor/Device</th>
<th>Company-Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Checkpoint</td>
</tr>
<tr>
<td>☐</td>
<td>Cisco</td>
</tr>
<tr>
<td>☐</td>
<td>Cisco Meraki</td>
</tr>
<tr>
<td>☐</td>
<td>Fortinet</td>
</tr>
<tr>
<td>☐</td>
<td>Juniper</td>
</tr>
<tr>
<td>☐</td>
<td>Palo Alto</td>
</tr>
<tr>
<td>☐</td>
<td>Other</td>
</tr>
</tbody>
</table>

Certificate-Based Firewall Access Method

<table>
<thead>
<tr>
<th>Vendor/Device</th>
<th>Company-Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Cisco</td>
</tr>
<tr>
<td>☐</td>
<td>Other</td>
</tr>
</tbody>
</table>

Step 2—Select a Regional Web Security Service IP Address

Required for the IPsec configuration. Your region dictates which IP address (or set of addresses) to enter. The format is: Estimated optimal region coverage (Data Center location). Select a primary and a secondary (for redundancy) location.

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

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

The Symantec Operations team maintains the following Knowledge Base article.

Step 3—Enter Network Information

<table>
<thead>
<tr>
<th>Network Item</th>
<th>Comments</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Where is this device’s location?</td>
<td></td>
</tr>
<tr>
<td>Preshared Key (VPN/Firewall only)</td>
<td>Required during device and Web Security Service configuration. Must be at least eight characters and cannot use special characters. Not required for cert-based firewall connections. PK:</td>
<td></td>
</tr>
<tr>
<td>AuthConnector IP Address</td>
<td>The domain controller where AuthConnector is to be installed.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Test Client/Subnet</td>
<td>You can send traffic from a test client without disrupting production traffic. IP/Subnet</td>
<td></td>
</tr>
<tr>
<td>Gateway (outside) IP Address</td>
<td>IP address used to communicate externally to the Web Security Service. IP address: Object name:</td>
<td></td>
</tr>
<tr>
<td>Internal Network IP Address/Object Interface</td>
<td>Internal network segment to be routed to the Web Security Service. IP address: Object name:</td>
<td></td>
</tr>
<tr>
<td>Internal Network IP Address/Object Interface</td>
<td>IP address: Object name:</td>
<td></td>
</tr>
<tr>
<td>Internal Network IP Address/Object Interface</td>
<td>IP address: Object name:</td>
<td></td>
</tr>
<tr>
<td>Internal Network IP Address/Object Interface</td>
<td>IP address: Object name:</td>
<td></td>
</tr>
</tbody>
</table>

Step 4—(Optional) Specify Groups of Interest

You can specify which groups or users (from your security Active Directory) are forwarded to the cloud service. This requires a manual editing of a config file, which is described in "Forward Specific User and Group Names to the Service" on page 175.

<table>
<thead>
<tr>
<th>Item</th>
<th>Comments</th>
<th>Values</th>
</tr>
</thead>
</table>
| Interest Group 1      | Group of interest sent to the Web Security Service. | Group Example: HQ-SALES\NAWest  
User Example: HQ-SALES\Administrator |
<table>
<thead>
<tr>
<th>Item</th>
<th>Comments</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interest Group 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interest Group 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interest Group 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interest Group 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interest Group 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interest Group 7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reference: Authentication IP Addresses

The Symantec Web Security Service Auth Connector communicates with devices in the geographically located data centers. The following are the list of authentication IP addresses by location.

The Symantec Operations team maintains the following Knowledge Base article.

Reference: IKE Encryption and Authentication Algorithms

Configuring a router device for the Symantec 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 Web Security Service supports the following combinations, with following caveat.

**Note:** Symantec did not test every combination. Although the expectation is these are supported, Symantec 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>
</tbody>
</table>
Firewall/VPN Access Method Guide: About Roaming Captive Portal/Page 28

### Keyword

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<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-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. Symantec 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 (Symantec recommends **AES128**).

e. Select an **ESP Authentication** option (Symantec 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 (PSK)" on page 35.

### Juniper SSG20 Devices

The Juniper SSG20 device-to-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 Screen]

a. **Name** the object. For example, **WSSEncryption**.

b. The **Authentication Method** option must be **Preshare**.

c. The **DH Group** (Diffie-Hellman) option can be **Group 2** or **Group 5**.

d. The **Encryption Algorithm** option can have a **3DES** or **AES** (128 or 256 bits) prefix.

e. The **Hash Algorithm** option can be **MD5** or **SHA1**.

f. Set the **Lifetime** value. The default value of **28800** seconds is acceptable.

g. 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 (PSK)"** on page 35.
Reference: Required Locations, Ports, and Protocols

Depending on your configured Symantec 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>Web Security Service IP addresses</td>
<td>199.19.250.192</td>
<td>portal.threatpulse.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>199.116.168.192</td>
<td>199.116.168.192</td>
<td></td>
</tr>
<tr>
<td>Firewall/VPN (IPsec)</td>
<td>80/443</td>
<td>IPsec/ESP</td>
<td>IPsec/ESP</td>
</tr>
<tr>
<td></td>
<td>500</td>
<td></td>
<td>UDP 500 (ISAKMP)</td>
</tr>
<tr>
<td></td>
<td>4500</td>
<td></td>
<td>UDP4500 if firewall is behind a NAT.</td>
</tr>
<tr>
<td>Proxy Forwarding</td>
<td>8080/8443</td>
<td>HTTP/HTTPS</td>
<td>Port 8080 to proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td>8084*</td>
<td></td>
<td>Port 8443 to proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*Port 8084 to proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*If this forwarding host is configured for local SSL interception.</td>
</tr>
<tr>
<td>Explicit Proxy</td>
<td>8080</td>
<td></td>
<td>PAC File Management Service (PFMS) pfm-s.wss.symantec.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://portal.threatpulse.com/pac">https://portal.threatpulse.com/pac</a></td>
</tr>
<tr>
<td>Access Method</td>
<td>Port(s)</td>
<td>Protocol</td>
<td>Resolves To</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trans-Proxy</td>
<td>No Default Route: 80, 443</td>
<td></td>
<td>ep.threatpulse.net:80 (no default route resolves to the following IP addresses.</td>
</tr>
<tr>
<td></td>
<td>One Common URL: 8080 (VPN Tunnel)</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></td>
<td></td>
<td>proxy.threatpulse.net:8080 (one common URL) resolves to any of the WSS data-center VIPs</td>
</tr>
<tr>
<td>Unified Agent</td>
<td>80</td>
<td>UDP (v4.9.1+), 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>443</td>
<td></td>
<td>Port 443 to ctc.threatpulse.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port 443 to client.threatpulse.net (DNS fallback)</td>
</tr>
<tr>
<td>MDM (registered iOS and Android devices)</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 Web Security Service 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>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>portal.threatpulse.com:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.192</td>
</tr>
</tbody>
</table>

### Auth Method

<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 to Active Directory</td>
<td>139,445</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>389</td>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3268</td>
<td>ADSI LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>135</td>
<td>Location Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AC-Logon App</th>
<th>80</th>
<th></th>
<th>Port 80 from all clients to the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML</td>
<td>8443 (over VPN)</td>
<td>Explicit and IPSec</td>
<td>to saml.threatpulse.net</td>
</tr>
<tr>
<td>Roaming Captive Portal</td>
<td>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: Egress IP Ranges

Protected traffic is tunneled through the Symantec 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.

Select a Firewall Device (PSK)

Configure the firewall device and the Web Security Service to use a preshared-key (PSK) to confirm the VPN-to-VPN connection. NAT-T is not supported with this method.

The following routing/firewall devices were tested and are supported by Symantec. You can attempt to configure other similar devices to perform a VPN-to-VPN connection to the Web Security Service. As new devices are vetted, they are added to this official documentation.

Tip: You can search the Symantec Knowledge Base for your device in question. Occasionally, other subject matter experts upload procedures that were not officially tested.

Pre-Deployment: Select Authentication Method

Before configuring a firewall device to send traffic to the Web Security Service, Symantec recommends deploying a user authentication method. This is required for user reporting and pre-traffic policy creation.

If you have not completed this task, refer to the Authentication information in the Web Security Service Access Methods or Solutions WebGuides/PDFs.

Pre-Shared Key/Standard Configuration

Select a vendor link below to begin the device configuration walkthrough.

- "Check Point Site-to-Site VPN Configuration (PSK)" on page 36
- "Cisco ASA Site-to-Site VPN Configuration (PSK)" on page 50
- "Cisco Meraki Firewall: Create a Site-to-Site VPN" on page 59
- "Fortinet Site-to-Site VPN Configuration (PSK)" on page 63
- "Juniper Site-to-Site VPN Connection (PSK)" on page 72
- "Palo Alto Site-to-Site VPN Configuration (PSK)" on page 82

Legacy Procedures

If you have an older model, Symantec previously provided device-specific procedures. These are now provided as legacy.

- Check Point (Simplified Mode)
- Cisco 1941
- Cisco ASA (Pre 8.3)
- Cisco ASA 8.3 or 8.4
- Fortinet with 4.x Firmware
- Juniper SSG20
Check Point Site-to-Site VPN Configuration (PSK)

Symantec tested and validated that Check Point® devices are able to forward web traffic to the Web Security Service for policy checks and malware scanning. The following procedure demonstrates the Simplified Mode with pre-shared secret method, which requires a unique gateway IP address (no NAT-T).

Version Demonstrated:
- Check Point Gateway running R77.30.
- Security Manager running R77.30.
- SmartConsole R77.30.
- EndPoint Security test with E80.50(8.3.937).

This procedure provides a guideline configuration that you can apply to the above model or other Check Point models. It is likely that you have an existing Check Point device configured in your network; therefore, slight alterations to the existing deployment might be required.

**Note:** R77.20 is the minimum supported version because of the Dead Peer Dead requirement.

**Deployment Notes**

- The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways.
- The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.
- You can create a designated host or subnet that tests the IPsec connectivity to the Web Security Service without interrupting the production traffic. After successful testing, you then add production subnets.

**Note:** Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

**Procedure**

**Prerequisite—Verify that the device is ready for configuration.**

This procedure assumes that the Check Point device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

**Step 1—Create Symantec Encryption Domain.**

Create a Simple Group of the five IP *Address Ranges* that define all Internet addresses. These ranges include loopback,
RFC1918, and Class D and E.

1. In the SmartDashboard, select **Network Objects**.

2. Right-click **Address Ranges** and select **Address Ranges > Address Range**.

   ![Network Objects](image)

   The interface displays the Address Range Properties dialog.

3. Define the first Internet range.

   ![Address Range Properties](image)

   a. **Name** the range.

   b. In the **First IP address** field, enter **1.0.0.0**.

   TRANS-PROXY ALTERNATIVE:
   - For Trans-Proxy deployments, refer to "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20 for options; then proceed to sub-step 5.

   c. In the **Last IP address** field, enter **9.255.255.255**.

   d. Click **OK**.

4. Repeat **Step 1.3** (above) four times to complete the Internet ranges.
a. First IP address: 11.0.0.0; Last IP address: 126.255.255.255.
b. First IP address: 128.0.0.0; Last IP address: 172.15.255.255.
c. First IP address: 172.32.0.0; Last IP address: 192.167.255.255.
d. First IP address: 192.169.0.0; Last IP address: 223.255.255.255.

5. Create the Simple Group. Remaining in the **Network Objects** applet, right-click **Groups** and select **Simple Group**. The interface displays the Group Properties dialog.

![Group Properties - Encryption_Domain](image)

a. Name the group.
b. From the **Not in Group** area, select the five range objects that you created in **Steps 1.3 and 1.4**.
c. Click **Add** to move them **In Group**.
d. Click **OK**.

**Step 2—Create the Local Encryption Domain.**

When a location is active, all outbound port 80 and 443 web traffic routes through the VPN tunnel to the Web Security Service. The following example identifies the subnets that you want sent to the service for processing.

**Tip:** Symantec assumes that this is an existing gateway device and that you have previously configured to send traffic to the Internet. If you do not have subnets configured, consult the documentation for the Check Point device.

1. In the **Network Objects** applet, right-click **Groups** and select **Simple Group**. The interface displays the Group Properties dialog.
a. **Name** the group.

b. From the **Not in Group** area, select internal subnets that transport Internet-bound traffic.

c. Click **Add** to move them **In Group**.

d. Click **OK**.

**Tip:** To perform Web Security Service testing, you can identify a single workstation to send rather than entire production subnets. When you are satisfied, edit the object to add the production subnets.

**Step 3—Exclude Non-Web Traffic (Protocol Ports)**

Create an protocol group that excludes the non-web protocols from inclusion in the VPN tunnel that connects to the Web Security Service.
1. In the SmartDashboard, select **Services**.

2. Right-click **Group** and select **New Group**. The interface displays the Group Properties dialog.

3. Click **New**. The interface displays the Group Properties dialog.
   
   a. **Name** the object. For example, indicate that these are ports 1 to 79.
   
   b. In **Port** field, enter **1-79**. This excludes all ports up to 80 (web).
   
   c. Click **Advanced**. The interface displays the Advanced TCP Service Properties dialog.
   
   d. Select **Match For 'Any'**. This prevents policy installation warnings because of a possible already-defined port.
   
   e. Click **OK**; click OK again to close the Group Properties dialog.

4. Repeat **Steps 3.1 through 3.3** to add two more groups.
   
   a. Mid-TCP-Ports: **81 to 442**.
   
   b. High-TCP-Ports: **444 to 65535**.
   
      This allows port 443 traffic into the VPN tunnel.

5. (Optional) You can also add ICMP and all UDP ports.

**Step 4—Define the Gateway.**

Create a Gateway (Interoperable Device) that points to the nearest Symantec datacenter for the configured location. Refer to your **planning sheet** for the datacenter IP address.
1. In the SmartDashboard, select **IPSec VPN** from the top ribbon.

2. From the left-menu, select **Gateways**.

3. From the **Gateway** options, click **+Add**. The interface displays the Interoperable Device dialog.
   a. Name the gateway.
   b. Enter the Web Security Service **IPv4 Address**.
   c. Click **OK**.

4. Add the Symantec Encryption Domain.
   a. Edit the new gateway.
   b. From the left-menu, select **Topology**.
   c. In the **VPN Domain** area, select **Manually Defined**.
   d. Click the browse icon-button (…) and select the Encryption Domain that you configured in **Step 1**.
   e. Click **OK**.

5. Add the Encryption Domain to Check Point gateway.
   a. From the left-menu, select **Gateways**.
   b. Select the configured Check Point gateway and click **Edit**. The interface displays the Check Point Gateway dialog.
   c. Select **Topology**.
d. Select the **External** interface.

e. In the **VPN Domain** area, select **Manually Defined**.

f. Click the browse icon-button (…) and select the Local Encryption Domain that you configured in Step 1.

g. Click **OK**.

**Step 5—Create the VPN Community**

Add the Check Point gateway and the Symantec device to participating gateways.

1. In the SmartDashboard, select **IPSec VPN** from the top ribbon.

2. From the left-menu, select **Communities**.

3. From the **Communities** options, select **New > Meshed Community**. The interface displays the Meshed Community Properties dialog.

   a. **Name** the community.

   b. Select **Participating Gateways**.
c. Click **Add**. The interface displays the Add Participating Gateways dialog.
d. The interface detects the available gateways. Select the Check Point gateway and the Web Security Service gateway that you created; click **OK**.
e. From the left-menu in the dialog, select **Tunnel Management**.
### Tunnel Management

**Permanent Tunnels**

- [ ] Set Permanent Tunnels
  - ( ) On all tunnels in the community
  - ( ) On all tunnels of specific Gateways
  - ( ) On specific tunnels in the community

- [ ] Enable Route Injection Mechanism (RIM)

**VPN Tunnel Sharing**

Control the number of VPN tunnels opened between:

- ( ) One VPN tunnel per each pair of hosts
- ( ) One VPN tunnel per subnet pair
- ( ) One VPN tunnel per Gateway pair

---

f. **Select** One VPN tunnel per Gateway pair.

**Warning:** Leaving this option at the default setting causes a substantial performance reduction.

g. From the left-menu in the dialog, select Advanced Settings > Excluded Service.
h. Click Add.

i. In the Add Service dialog, scroll to and select the Excluded Protocols object that you created in Step 3.

j. Click OK.

4. Establish the pre-shared key (PSK). Remaining under Advanced Settings, select Shared Secret.
a. The dialog contains the Web Security Service peer that you configured. Select it and click **Edit**.

b. Enter the pre-shared key **(Secret)** used to by the Web Security Service to authenticate the tunnel and click **Set**. Refer to your planning sheet.

![Tip: The PSK must be at least eight characters and cannot use special characters.](image)

c. Click **OK**.

5. Select the Internet Key Exchange algorithm and disable NAT-T. Remaining under **Advanced Settings**, select **Advanced VPN Properties**.

![Advanced VPN Properties](image)


b. Verify that **Disable NAT inside the VPN community** is selected.

c. Click **OK**.

### Step 6—Enable Dead-Peer-Dead.

To avoid datacenter connection issues, you must enable Dead-Peer-Dead on the Check Point device. You cannot accomplish this through the SmartDashBoard. You must use the Check Point Database Tool (GuiDBedit).

1. Access the GuiDBedit program, which is located in the SmartConsole **PROGRAM** folder.
   a. For example, on Windows, the default path to navigate to is:

   `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.30\PROGRAM`

   b. Run the **GuiDBedit** program.

2. In the database tool, set Dead Peer Dead only on the Web Security Service gateway object(s).
a. In the Tables tab, select Network Objects > Network Objects.

b. Scroll through Object Names to locate the Web Security Service gateway object that you created.

c. Scroll through the Field Names to locate tunnel_keepalive_method.

d. Double-click dpd and enable it.

e. Save the database tool changes.

3. Return to the SmartDashboard and Install the policy.

Step 7—Exclude Auth Connector Traffic from the Web Security Service.

If Auth Connector traffic requires access to the Internet through the Check Point gateway, you must exclude that traffic from routing to the Web Security Service. Many datacenters have several to many Auth IP addresses. This step describes how exclude subnets verses manually configuring individual addresses.

Tip: If your Access Method is Trans-Proxy (IPsec over VPN), you can skip this step.

1. In the SmartDashboard, select Network Objects.

2. Right-click Networks and select Network.
The interface displays the Network Properties dialog.

3. Define the first Internet range.

![Image of Network Properties dialog]

**Network Properties - Auth_Chicago**

- **Name**: Auth_Chicago
- **Comment**: Exclude these from the cloud service
- **Network Address**: 198.135.124.128
- **Net Mask**: 255.255.255.224

- **Tip**: For a list of authentication addresses per datacenter, see "Reference: Authentication IP Addresses" on page 26.

4. Add this object to the Excluded Domains object that you created in **Step 2**.
Next Selection

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.
- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Cisco ASA Site-to-Site VPN Configuration (PSK)

Symantec tested and validated that Cisco® router devices are able to forward web traffic to the Web Security Service for policy checks and malware scanning. The following procedure demonstrates the pre-shared secret method, which requires a unique gateway IP address (no NAT-T).

Version Demonstrated:
- ASA5510
- Cisco ASDM 7.1(1)

This procedure provides a guideline configuration that you can apply to the above model or other Cisco models. It is likely that you have an existing Cisco device configured in your network; therefore, slight alterations to the existing deployment might be required.

Deployment Notes

- The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways.
- The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.
- You can create a designated host or subnet that tests the IPsec connectivity to the Web Security Service without interrupting the production traffic. After successful testing, you then add production subnets.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Procedure

Prerequisite—Verify that the router is ready for configuration.

This procedure assumes that the Cisco ASA device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

1. Select the Configuration > Interfaces > Switch Ports tab.
2. Verify the list has one interface is required for the outside (Web Security Service) connection and as many available interfaces for inside routes (see planning sheet).

Step 1—Create a site-to-site connection profile.

1. Access the Connection Profile dialog.
a. Select **Configuration**.

b. Click **Site-to-Site VPN**.

c. Select **Enable inbound VPN sessions**....

d. In the **Connection Profiles** area, click **Add**. The device displays the Add IPsec Site-to-Site Connection Profile dialog.

2. Configure the IPsec site-to-site connection profile.
a. Select the Peer IP Address: Static option and enter the regional Web Security Service primary IP address for this location (refer to your planning sheet). The Connection Name (selected by default) automatically fills in the same information.

b. For the Interface option, select outside.

c. For the Protected Networks: Local Network option, select inside-network

d. The Protected Networks: Remote Network setting depends on the Access Method:
   - For stand-alone deployments, select any.
   - For Trans-Proxy deployments, refer to “About Trans-Proxy (Explicit Proxy Over IPsec)” on page 20 for options.

e. Enter the Pre-shared Key, which is the string used to secure the encrypted tunnel between the router and the Web Security Service (eight-character minimum; refer to your planning sheet).

Tip: The PSK must be at least eight characters and cannot use special...
f. Remain in the IPsec Site-to-Site Connection Profile dialog and proceed to Step 3.

3. In the left pane, select Advanced > Crypto Maps.

![IPsec Site-to-Site Connection Profile dialog](image)

a. Enable the Perfect Forward Secrecy option.
b. For Diffie-Hellman Group, select group5.
c. Clear the NAT-T option.
d. Click OK.

4. Still in the Add IPsec Site-to-Site Connection Profile, click IKE Policy: Manage. The device displays the Configure IKE v1 Policies dialog.
The recommended **Encryption Algorithm: IKE Policy** values have top-level (or high) priority. The Web Security Service supports many combinations. See See "Reference: IKE Encryption and Authentication Algorithms" on page 27.

a. **Edit** an existing policy or **Add** a new one. The device displays the IKE Policy dialog. Select the recommended parameters.

b. For **Authentication**, select **pre-share**.

c. Select an **Encryption** value.

d. For **D-H Group** (Diffie-Hellman), select **5**.

e. Select a **Hash** value.

f. Set the **Lifetime** value to under 4 hours (14400 seconds).

g. Click **OK** in both dialogs to close.

h. Remain in the IPsec Site-to-Site Connection Profile dialog.

5. The Cisco device-to-Web Security Service access method requires selecting a supported **IPsec Proposal**. Cisco references groups of these as *transform sets*. Click **Advanced > IPsec Proposal**.
a. **Edit** an existing policy or **Add** a new one. The device displays the IKE Policy dialog. Select the recommended parameters.

b. **Name** the proposal so that you can identify it in a long list. For example, **Cloud_AES256SHA**.

c. For **Mode**, select **Tunnel**.

d. Select an **ESP Encryption**.

e. Select an **ESP Authentication**.

f. Click **OK** in both dialogs to close.

g. **Remain** in the IPsec Site-to-Site Connection Profile dialog.

6. Click **OK** to create the Connection Profile, which should look similar to this:

---

**Step 2—Create the IPsec connection rule for HTTP and HTTPS traffic.**

1. Select **Configuration > Site-to-Site VPN > Crypto Maps**. You must modify **Service** to include the **HTTP** and **HTTPS** protocols.
1. Select the Crypto Map that you configured in Step 1.5.
   a. Click Edit. The device displays the Edit IPsec Rule dialog.

2. On the **Tunnel Policy (Crypto Map) - Basic** tab, verify that the configuration information was automatically copied from Step 1.

3. Set the **Destination Criteria: Service** protocols to HTTP and HTTPS.
   a. Select the **Traffic Selection** tab.
   b. For **Service**, click the browse icon. The device displays the Browse Service dialog.
   c. Add the Scroll the list or Filter to HTTP and HTTPS.
   d. Select them and click **Service** to add them to this policy.
   e. Click **OK**. The completed Crypto Map should look similar to the following
4. Navigate to **Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Policy.** Verify that the **Use the configured rules to match a certificate to a Connection Profile** option is cleared.

![Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Policy]

**Step 3—Create Firewall NAT Rules (HTTP and HTTPS) that Forward Traffic to the Web Security Service.**

1. Select **Configuration > Firewall > NAT Rules.**
2. Click **Add** and select **Add NAT Rule Before "Network Object" NAT Rules.**
3. Define the HTTP rule.

![Configuration > Firewall > NAT Rules]

a. Set the **Source Address** option to **Any.**

**Tip:** To test the Web Security Service connectivity before adding all users, enter a single IP address of a client system that has web access from your network.
egress point. After successful testing, return to this configuration and change to Any.

b. Set the Service option to the HTTP service object that you created in Step 2.3.

c. Click OK.

4. Repeat the above sub-step 3 to create a NAT rule for the HTTPS service object.

The completed rules should look similar to the following.

```
<table>
<thead>
<tr>
<th>Match Criteria: Original Packet</th>
<th>Action: Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Intf</td>
<td>Dest Intf</td>
</tr>
<tr>
<td>inside</td>
<td>outside</td>
</tr>
<tr>
<td>original packet</td>
<td>original packet</td>
</tr>
<tr>
<td>destination</td>
<td>destination</td>
</tr>
<tr>
<td>previous packet</td>
<td>next packet</td>
</tr>
<tr>
<td>service</td>
<td>service</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>No Proxy</td>
<td>No Proxy</td>
</tr>
</tbody>
</table>
```

**Step 4—Verify the WSS Service Connection**

To verify the IPsec site-to-site tunnel connection, select Monitoring > VPN > VPN Statistics > Sessions.

If either of these steps produces an unsuccessful result, retract your configuration steps.

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.

- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Cisco Meraki Firewall: Create a Site-to-Site VPN

Like other vendor firewalls, you configure the Cisco Meraki firewall to perform a Site-to-Site VPN connection to the Web Security Service. However, Meraki firewalls always forces NAT-T even when the device connects directly from a public IP address. Furthermore, Meraki firewalls do not support certificates. Therefore, the procedure to route web traffic to the Web Security Service differs from other vendors.

Deployment Notes

- The Web Security Service is a third-party peer, which means the settings are organization-wide.
- Use of the Meraki firewall Access Method requires the All Ports license.
- Firewalls belonging to the same organization (account in their cloud portal) cannot have the overlapping ACL destination networks. To forward all internet traffic to the Web Security Service, you must configure the ACL subnet to 0.0.0.0/0. This leads to following restrictions.
  - There can only be one third-party peer (the datacenter VIP) configured in an organization.
  - All Meraki firewalls in the organization can talk to that one datacenter only.
  - All Meraki firewalls in the organization must use the same pre-shared key (PSK). So these sites should be configured in the WSS portal with the same PSK.
  - Because there can be only datacenter VIP configured in the organization, you cannot configure second datacenter for failover purposes.
  - Because all Meraki firewalls in the organization will connect to the single third-party peer (DC) configured in the organization, you must add a Location for each Meraki firewall.
- To work around some of the limitations above, separate your firewalls across multiple organizations.
- Do not send Auth Connector traffic to the Web Security Service.
- You can create a designated host or subnet that tests the IPsec connectivity to the Web Security Service without interrupting the production traffic. After successful testing, you then add production subnets.

**Note:** Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. *The screenshots in the following procedure might not reflect this advisory.*

Prerequisites

- At least one Meraki firewall is deployed as a security device.
- Based on the deployment notes above, determine if you are configuring a single Meraki device for all connections or deploying a Meraki device in multiple geographical locations as required for your network security architecture.
- Have access credentials to the Meraki cloud-based interface.
- Know the subnet (local network) that is to connect to the Web Security Service.
- Identify and record the VIP of the closest Web Security Service datacenter (refer to your planning sheet).
Procedure

1. Access the Meraki web-based interface: https://dashboard.meraki.com; log in.
2. Select Security Appliance > Configure > Site-to-Site VPN.
3. Select a network.
   - If you have a single existing network that already applies to the traffic that will route to the Web Security Service, proceed to the next step.
   - If you have multiple existing networks: From the Network drop-down list, select an existing network to configure.
   - You want to create a new network that applies to another static route.

   **Tip:** This requires an unassigned device and its serial number.

   a. From the Network drop-down list, select Create a New Network. The interface displays the network creating screen.
   b. Name the network.
   c. For Network Type, select Security Appliance.
   d. Accept the Default Meraki Configuration.
   e. Click Add Devices; complete the on-screen instructions.
   f. Click Create Network.
   g. Return to the Security Appliance > Configure > Site-to-Site VPN screen.

4. Return to the Security Appliance > Configure > Site-to-Site VPN screen.
5. In the Site-to-Site VPN > Type area, select Hub (Mesh). This expands the screen to more VPN parameters.
6. Set the VPN settings.
Firewall/VPN Access Method Guide: Cisco Meraki Firewall: Create a Site-to-Site VPN

7. Define the Non-Meraki VPN peer, which is the Web Security Service datacenter.

**Tip:** Remember, you *must* use the same VIP for all of your Meraki configurations. You cannot connect to multiple datacenters.

![Organization-wide settings](image)

a. **Name** the peer. Because this is the Web Security Service datacenter location, consider using a geological name.

b. Enter the Web Security Service datacenter **Public IP** (VIP).

**TRANS-PROXY ALTERNATIVE:**

- For Trans-Proxy deployments, refer to "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20 for options; then proceed to sub-step 5.

c. The **Private Subnet** must be **0.0.0.0/0**.

d. Accept the **Default IPsec Policies**.

e. Enter the **Preshared Secret** key (PSK) used to by the Web Security Service to authenticate the tunnel. Refer to your planning sheet.

**Tip:** The PSK must be at least eight characters and *cannot* use special characters.
8. Accept the default **Site-to-Site Inbound** and **Outbound** firewall rules. The outbound rule must allow all; the inbound rule cannot be changed.

9. Click **Save Changes**.

**Monitoring the VPN**

After you create a Location in the Web Security Service portal (Next Selection below) and the Meraki device begins to communicate with the cloud service, you can return to the interface monitor the status of the VPN connection.

- Select **Security Appliance > Monitor > VPN Status**.

Next Selection

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.

- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Fortinet Site-to-Site VPN Configuration (PSK)

Symantec tested and validated that Fortinet® firewall devices are able to forward web traffic to the Web Security Service for policy checks and malware scanning. The following procedure demonstrates the pre-shared secret method, which requires a unique gateway IP address (no NAT-T).

Version Demonstrated:
- Fortinet 300C
- v5.2.1, build618 (GA)

This procedure provides a guideline configuration that you can apply to the above model or other Fortinet models. It is likely that you have an existing Fortinet device configured in your network; therefore, slight alterations to the existing deployment might be required.

Deployment Notes

- The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways.
- The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.
- You can create a designated host or subnet that tests the IPsec connectivity to the Web Security Service without interrupting the production traffic. After successful testing, you then add production subnets.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Procedure

Prerequisite—Verify that the device is ready for configuration.

This procedure assumes that the Fortinet device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

STEP 1—Begin a Custom VPN Tunnel configuration.

1. From the left-menu, select VPN > Tunnels.
2. Click Create New.
3. The interface displays the VPN Setup screen. Define the Phase 1 tunnel.
a. Enter a meaningful **Name** for the tunnel interface. For example, the location of the device.

b. Select **Custom VPN Tunnel (No Template)**.

c. Click **Next**. The interface displays a page with numerous network configuration parameters.

**STEP 2—Define the tunnel network parameters.**

**Tip:** If a parameter change is not described here, the default is acceptable.

1. Enter the following network and connection authentication information.
a. From your planning sheet, enter the Web Security Service IP Address.

**TRANS-PROXY ALTERNATIVE:**

- For Trans-Proxy deployments, refer to "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20 for options; then proceed to sub-step 5.

b. Select the Interface that provides the outside connection.

c. Enter the Pre-shared Key, which is the string used to secure the encrypted tunnel between the router and the Web Security Service (eight-character minimum; refer to your planning sheet).

    Tip: The PSK must be at least eight characters and cannot use special characters.

2. Scrolling down displays the Phase 1 Proposal area.

Leave the Local ID field blank. By default, this value is auto. An added value might cause the tunnel to fail because of a FQDN interruption.

The final area on the screen is New Phase 2.

If the device did not populate the Name field, enter the meaningful name.

The Local Address value(s) tell the device which internal segments to route to the outside and thus to the Web Security Service.
- If you are performing a test, you can select IP Address from the drop-down and enter a single client IP.
- If you are ready to add production traffic, select Subnet and enter the IP address and subnet information.

c. Click Advanced to display additional configuration options.

4. Select Perfect Forward Secrecy (PFS), as this is a required option. Show screen...

---

**Step 3—Create backup tunnel.**

(Optional, but recommended) For failover, repeat Steps 1 and 2 to create backup VPN tunnel that directs traffic to another regional Web Security Service datacenter. When complete, the device displays VPN configurations similar to the following.

---

**Step 4—Route Web Security Service-bound traffic through the tunnel interfaces.**

1. Select Router > Static Routes.
2. Click Create New. The device displays the New Static Route page.
3. From the Device drop-down list, select the primary Web Security Service location that you configured in Step 2.1.a.

---
4. If you defined a backup location, repeat sub-steps 4.2 and 4.3 above to add that location. When complete, the device displays locations similar to the following.

![Image of device displaying locations]

**Step 5—Define policy routes.**

1. Select **Router > Policy Routes**.
2. Click **Create New**. The device displays the New Routing Policy page.
3. Route port 80 traffic to the primary Web Security Service tunnel interface.

![Image of policy route configuration]

**If incoming traffic matches:**

- **Protocol**: TCP
- **Incoming interface**: Internal
- **Source address / mask**: 192.168.42.22 / 0.0.0.0
- **Destination address / mask**: 0.0.0.0
- **Source Ports**: From: 1 To: 65535
- **Destination Ports**: From: 80 To: 80
- **Type of Service**: Bit Pattern 0x00 Bit Mask 0x00

**Then:**

- **Action**: Forward Traffic
- **Outgoing interface**: WSS_WestCoast
- **Gateway Address**: 0.0.0.0
- **Comments**: Write a comment...

a. For the **Protocol**, select TCP.
b. From the **Incoming Interface** drop-down list, select the internal object (traffic coming from internal sources).
c. Enter the **Source Address/Mask** test IP address or production IP address and subnet.
d. For the **Destination Address/Mask**, enter `0.0.0.0/0`, which equals traffic sent to any destination.

e. For the **Destination Ports**, enter **80** to **80**. This designates web (HTTP) traffic.

f. From the **Outgoing Interface** drop-down list, select the primary Web Security Service location.

g. Click **OK**.

4. Repeat sub-steps 5.2 and 5.3 to create the a route with the same parameters, but in the **Destination Ports** fields, enter **443**, which designates secure web (HTTPS) traffic.

```
<table>
<thead>
<tr>
<th>Source Ports</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Ports</td>
<td>4</td>
<td>443</td>
</tr>
<tr>
<td>Type of Service</td>
<td>Bit Pattern</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td>Bit Mask</td>
<td>0x00</td>
</tr>
</tbody>
</table>
```

5. Repeat sub-steps 5.2 and 5.3 to create HTTP (port 80) and HTTPS (port 443) policy routes for the backup tunnel interface (if you are configuring one).

**Tip:** The order of the entries is important. The primary tunnel must be listed above the secondary tunnel.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>internal</td>
<td>WSS_WestCoast</td>
</tr>
<tr>
<td>6</td>
<td>internal</td>
<td>WSS_WestCoast</td>
</tr>
<tr>
<td>7</td>
<td>internal</td>
<td>WestCoast2nd</td>
</tr>
<tr>
<td>8</td>
<td>internal</td>
<td>WestCoast2nd</td>
</tr>
</tbody>
</table>

**Note:** If you employing SAML authentication, you must also create an additional policy route for **Destination Port 443**.

**Step 6—Define firewall policies that allow traffic through the tunnel interface.**

1. Select **Policy & Objects > IPv4**.

2. Click **Create New**. The device displays the New Policy page.

3. Define the following policy options.
From the **Incoming Interface** drop-down list, select **internal**.

b. From the **Source Address** drop-down list, select **internal_subnet**.

c. From the **Outgoing Interface** drop-down list, select the primary Web Security Service location.

d. From the **Destination Address** drop-down list, select **all**.

e. The default **Schedule** is **always** (applies).

f. From the **Service** drop-down list, select HTTP (in the **Web Access** section).

g. Click the + icon to add another **Service** drop-down list; select **HTTPS**.

h. Verify that **NAT** is disabled.

i. Click **OK**.

**Tip:** In the example, only HTTP and HTTPS protocols are allowed over the VPN tunnel interfaces. If both VPN interfaces are down, then HTTP and HTTP traffic triggers the permit rule on the **wan1** interface and web traffic goes direct to the Internet. If you have a requirement that web traffic must be denied if both tunnel interfaces are down, and additional rule on **internal-wan1** to deny that traffic.

**Step 7—Optional Failover Configuration**

Symantec testing indicates that Data Center failover is provided without any additional configuration.
If a Web Security Service data center location IP address becomes unresponsive, the Fortinet device takes the appropriate interface down and the route policies will not apply. The next route policies are used instead, which sends traffic to the backup data center.

Fortinet provides an optional setting for the backup interface to monitor the primary. Testing did not indicate a difference in failover results when set, but you can set this option. Follow the commands in the Fortinet CLI example to setup monitoring.

```
FG80CM # config vpn ipsec phase1-interface
FG80CM # [phase1-interface] # edit WestCoast2nd
FG80CM # [WestCoast2nd] # set monitor WSS_WestCoast
```

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.
- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Juniper Site-to-Site VPN Connection (PSK)

Symantec tested and validated that Juniper® devices are able to forward web traffic to the Web Security Service for policy checks and malware scanning. The following procedure demonstrates the pre-shared secret method, which requires a unique gateway IP address (no NAT-T).

Version Demonstrated:
- SRX100h
- Requires JUNOS Software Release [10.0R1.8] or later

This procedure provides a guideline configuration that you can apply to the above model or other Juniper models. It is likely that you have an existing Juniper device configured in your network; therefore, slight alterations to the existing deployment might be required.

Deployment Notes

- The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways.
- The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.
- You can create a designated host or subnet that tests the IPsec connectivity to the Web Security Service without interrupting the production traffic. After successful testing, you then add production subnets.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Procedure

Prerequisite A—Verify that the router is ready for configuration.

a. Select Configure > Interfaces.
   
b. Verify the list has as many interface pairs as required, plus the management interface.

Step 1—Create a Phase I proposal

1. Select Configure > IPsec VPN > Auto Tunnel > Phase I.
   
2. Click Add. The device displays the Add Proposal/IKE Proposal dialog.
   
3. Define the proposal.

a. **Name** the proposal.

b. **Authentication Algorithm**—Select a supported value; for example, sha256.

c. **Authentication Method**—Select pre-shared-keys.

d. (Optional) Enter a **Description** the proposal. A descriptive name allows others in your organization to know the purpose.

e. **Diffie-Hellman (DH) Group**—Select a supported group; for example, group5.

f. **Encryption Algorithm**—Select a supported value; for example, aes-218-cbc.

g. **Lifetime seconds**—Set to 48000.

h. Click **OK**.

**Step 2—Define the IKE Policy.**

1. On the **Configure > IPsec > VPN > Auto Tunnel > Phase I** page, click the **IKE Policy** tab.

2. Click **Add**. The device displays the Add Policy/IKE Policy dialog/tab.

3. Configure the IKE policy to use the cloud phase 1 proposal defined in Step 1.
a. **Name** the policy.

b. **Mode**—Select **main**.

c. Select **User Defined**; select the **P1 Proposal** from **Step 1** and click the arrow to move it to the **Selected** list.

4. Define the pre-shared key, which is the string that validates the encrypted tunnel between the router and the Web Security Service (refer to your planning sheet).
a. Click the IKE Policy Options tab.

b. Select Pre Shared Key.

c. Select Ascii text and enter the key.

**Tip:** The PSK must be at least eight characters and cannot use special characters.

d. Click OK.

### Step 3—Create a Site to Site Tunnel gateway. You must also enable Dead Peer Detection and disable NAT Traversal.

1. On the Configure > IPsec > VPN > Auto Tunnel > Phase I page, click the IKE Gateway tab.
2. Click Add. The device displays the Add Gateway/IKE Gateway dialog/tab.
3. Configure the gateway to use the IKE policy from Step 2.

   a. Name the gateway.
   
   b. Select the IKE Policy that you defined in **Step 2**.
   
   c. Select which External Interface connects to the Web Security Service.
   
   d. Select Site to Site Tunnel.
   
   e. Enter the primary Web Security Service IP Address. Refer to your planning sheet.
TRANS-PROXY ALTERNATIVE:

- For Trans-Proxy deployments, refer to "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20 for options; then proceed to sub-step 5.

  f. For the **Local ID**, select **IP Address** and enter the SRX device's external IP address.

4. Enable Dead Peer Detection and disable NAT Traversal.

    a. Click the **IKE Gateway Options** tab.
    b. Select **Dead Peer Detection**. Select **Always send**. Set the **Interval** value to 10 and the **Threshold** value to 5.
    c. Select **NAT-Traversal**: **Disable**.
    d. Click **OK**.

**Step 4—Define the cloud connection proposal (Phase 2) connection.**

1. Select **Configure > IPsec VPN > Dynamic VPN > IPSec Autokey**.
2. Click **Add**. The device displays the **Configure > Dynamic VPN** page.
3. Set the dynamic Phase 2 parameters.
a. **Name** the Phase 2 proposal.

b. (Optional) Enter a **Description** the proposal. A descriptive name allows others in your organization to know the purpose.

c. **Authentication Algorithm**—Select **hmac-sha1-96**.

d. Symantec recommends **3des-cbc** for the **Encryption Algorithm**.

e. **Lifetime kilobytes**—Symantec recommends 1000000.

f. **Lifetime seconds**—Symantec recommends 48000.

g. **Protocol**—Select **esp**, which ensures privacy (encryption) and source authentication and content integrity (authentication).

h. Click **OK**.

**Step 5—Define the IPsec policy.**

1. Click the **IPSec Policy** tab.

2. Click **Add**. The device displays the **Configure > Dynamic VPN** page.

3. Define the policy.
a. **Name** the policy.

b. (Optional) Enter a **Description** the proposal. A descriptive name allows others in your organization to know the purpose.

c. **Perfect Forward Secrecy**—Symantec recommends **group5**.

d. For the **Proposal**, select **User Defined** and select the proposal you defined in **Step 4**.

e. Click **OK**.

**Step 6—Create the IPsec gateway.**

1. Click the **IPSec AutoKey** tab.
2. Click **Add**. The device displays the **Configure > Dynamic VPN** page.
3. Configure the VPN connection to use the cloud gateway and VPN policy.
a. **Name** the VPN.

b. **Remote gateway**—Select the gateway you created in Step 3.

c. **IPSec policy**—Select the gateway you created in Step 5.

d. **Establish tunnels**—Select on-traffic. This option consumes fewer resources, as tunnels are established only when needed.

e. Click **OK**.

**Step 7—Define policy that routes HTTP traffic to the Web Security Service.**

1. Select **Configure > Security > Policy > FW Policies**.

2. Click **Add**. The device displays the Add Policy/Policy page.

3. Create policy that routes HTTP traffic to the Web Security Service.
a. **Name** the policy.

b. **From Zone**—Select trust.

c. **To Zone**—Select untrust.

d. **Source Address**—Select all applicable subnets —or— if you created a **Policy Element** that contains your internal subnets, select it.

e. **Destination Address**—Select any.

f. **Application**—Select junos-http. This is the default element that includes TCP traffic on port 80.
g. **Policy Action**—Select **permit**. When you select this, the SRX interface displays the **Permit Action** tab. Proceed to the next step to complete the policy.

4. Select the Web Security Service VPN profile that you created in **Step 6.3**.

5. Click **OK**.

**Step 8—Repeat Step 7 for the HTTPS protocol.**

In **Step 7.3.f**, select **junos-https**.

**Failover Config**

If you are sending traffic to Singapore, which currently requires two IP address configurations, or you want to provide a layer of failover for other connection issues, use the CLI to add the following:

```
set security ike gateway BC_Cloud_Gateway secondary_cloud_IP
```

The output is:

```
gateway cloud_access_ike_gateway {
  ike-policy BC_Cloud_Gateway;
  address [ primary_cloud_IP secondary_cloud_IP ];
}
```

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.

- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Palo Alto Site-to-Site VPN Configuration (PSK)

Symantec tested and validated that Palo Alto® firewall devices are able to forward web traffic to the Web Security Service for policy checks and malware scanning. The following procedure demonstrates the pre-shared secret method, which requires a unique gateway IP address (no NAT-T).

Version Demonstrated:
- Palo Alto 200
  - Version 5.0.6 is the required minimum.

This procedure provides a guideline configuration that you can apply to the above model or other Palo Alto models. It is likely that you have an existing Palo Alto device configured in your network; therefore, slight alterations to the existing deployment might be required.

Deployment Notes

- The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways.
- The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.
- You can create a designated host or subnet that tests the IPsec connectivity to the Web Security Service without interrupting the production traffic. After successful testing, you then add production subnets.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Procedure

Prerequisite—Verify that the device is ready for configuration.

This procedure assumes that the Palo Alto device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

STEP 1—Create a Tunnel Interface.

1. Select Network > Interfaces > Tunnel.
2. Create a tunnel interface on the default virtual router that egresses Internet traffic. Click Add. The device displays the Tunnel Interface dialog.
a. Name the interface. Enter an **Interface Name** and a subsequent number. For example, if you enter `tunnel1` and 1, the Interface name becomes `tunnel.1`.

b. Select **IPv4**.

c. Click **Add**; enter an internal IP address that the Palo Alto device uses to monitor policy-based routing rules that send network traffic over tunnels.

d. Click **OK**.

3. (Optional) For failover, repeat sub-steps 1 and 2 to add a second address.

### STEP 2—Create a Zone for tunneled traffic.

1. Select **Network > Zones**.

2. Click **New**. The device displays the Zone dialog.
a. Name the Zone. For example, **WSS_Zone**.
b. Select **Layer 3** as the **Type**.
c. Add the tunnel(s) that you created in **Step 1**.
d. Click **OK**.

**STEP 3—Create an IKE crypto profile.**


1. Select **Network > Network Profiles > IKE Crypto**.
2. Click **New**. The device displays the Zone dialog.
a. **Name** the Profile. For example, **WSS_IKE_Crypto**.

b. **Add** the DH Group. Symantec recommends **group 5**.

c. **Add** the Encryption algorithm. Symantec recommends **aes128**.

d. **Add** the Authentication algorithm. Symantec recommends **md5**.

e. **Add** the Lifetime value. Symantec recommends **28000 Seconds**, which is eight (8) hours; do not exceed **86400** seconds or 24 hours.

f. Click **OK**.

**STEP 4—Create an IPSec crypto profile.**

1. Select **Network > Network Profiles > IPSec Crypto**.

2. Click **New**. The device displays the Zone dialog.
a. Name the Profile. For example, **WSS_IPSec_Crypto**.
b. From the **IPSec Protocol** drop-down, select **ESP**. This option ensures privacy (encryption), content integrity (authentication), and source authentication.
c. Add the **DH Group**. Symantec recommends **group 5**.
d. Add the **Encryption** algorithm. Symantec recommends **3des-cbc**.
e. Add the **Authentication** algorithm. Symantec recommends **sha1**.
f. Add the **Lifetime** value. Symantec recommends **3600 Seconds**, but do not exceed **14400** or four hours.
g. Add the **Lifesize** value. Symantec recommends **1000 MB**.
h. Click **OK**.

**STEP 5—Create an IKE gateway.**

1. Select **Network > Network Profiles > IKE Gateway**.
2. Click **Add**. The device displays the IKE Gateway dialog.

![IKE Gateway](image)

**IKE Gateway**

- **a. Name**: WSS_IKE_Gateway_1
- **b. Interface**: ethernet/1
- **c. Local IP Address**: 10.9.46.146/22
- **Peer IP Address**: 199.19.248.164
- **e. Pre-shared Key**: ********
- **f. Local Identification**: IP address 192.168.100.22
- **g. Peer Identification**: IP address 199.18.248.164

a. Name the Gateway. For example, **WSS_IKE_Gateway_1**.
b. Select the gateway-facing **Interface**.
c. Enter the outgoing **Local IP Address** (or you can leave this field blank if only one exists).
d. Enter the first Web Security Service **IP Address** (refer to your planning sheet).

**TRANS-PROXY ALTERNATIVE:**

- For Trans-Proxy deployments, refer to "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20 for options; then proceed to sub-step 5.

e. Enter the **Pre-shared Key**, which is the string used to secure the encrypted tunnel between the router and the Web Security Service (eight-character minimum; refer to your planning sheet).
f. From the **Peer Identification** drop-down, select **IP Address** and enter the gateway IP address.

g. From the **Local Identification** drop-down, select **IP Address** and enter the same **Peer IP Address** that you entered in step d.

h. Remain in this dialog and proceed to the sub-step 3.

3. Select **Show Advanced Phase 1 Options**.

![Advanced Phase 1 Options](image.png)

a. From the **Exchange Mode** drop-down, select **main**.

b. Select the **IKE Crypto Profile** that you defined in Step 3.

c. Verify that **Enable Passive Mode** option is clear.

d. Verify that the **Enable NAT Traversal** option is clear.

e. Select **Dead Peer Detection**.

f. Click **OK**.

4. (Optional) For failover, repeat sub-steps 2 and 3 and configure a second IKE Gateway set to another Symantec datacenter.

**STEP 6—Create an IPSec tunnel.**

1. Select **Network > IPSec Tunnels**.

2. Click **Add**. The device displays the IPSec Tunnel dialog.
a. **Name** the Tunnel. For example, **WSS_Tunnel_1**.

b. Select the **Tunnel Interface** that you created in **Step 1**.

c. Select the **IKE Gateway** that you created in **Step 5**.

d. Select the **IPSec Crypto Profile** that you created in **Step 4**.

e. For failover, select **Show Advanced Options**.

f. Select a failover profile.

   i. Select **Tunnel Monitor**.

   ii. Enter the **Destination IP**, which is the Symantec datacenter IP.

   iii. Select the monitor **Profile** that contains the failover option: **Wait Recover** or **Fail Over** to the secondary location.

   

**Note:** If the device does not yet have such a profile, go to **Network > Network Profiles > Monitor**.

3. Create a **Proxy ID** for the tunnel. In a normal site-to-site (non-cloud) VPN, you likely create one ProxyID for each subnet or service that requires access the VPN. However, you can only create only one ProxyID for the Web Security Service configuration. Therefore, ensure that this ProxyID includes all subnets to be routed to the Web Security Service. Alternatively, you can create multiple VPN tunnels.
a. Click the **Proxy IDs** tab.

b. Click **Add**. The device displays the Proxy ID dialog.

c. Name the **Proxy ID**. For example, **WSS_Tunnel_1_proxy**.

d. Enter the **Local** subnet that will send traffic in the tunnel to the Web Security Service.

e. Click **OK**.

4. Click **OK**.

**STEP 7—Define a security rule that allows traffic to the Web Security Service.**

1. Select **Policies > Security**.

2. Click **Add**. The device displays the Security Policy Rule dialog.

3. On the **General** tab, **Name** the rule.

4. Add the source zone.
5. Add the destination zone.

a. Click the **Destination** tab.

b. Click **Add** and select the **zone** that you created in **Step 2**.
6. Add the allowed services.

   ![Security Policy Rule](image)

   a. Click the **Service/URL Category** tab.

   b. Add services.

      - For stand-alone IPSec deployments, click **Add** and select **service-http** and **service-https**; if you plan to configure the Web Security Service to perform SAML authentication over IPSec tunnels, select **service-saml**.

      ![Note](image)

      **Note**: If the **service-saml** object is not present, you must create the object. Add a new service that sends TCP traffic destined to port 8443 over the tunnel.

      - For trans-proxy deployments, add only **service-http**, which is port 80 traffic.

   7. Click **OK**.

**STEP 8—Create a rule that disables NAT for traffic routing to the Web Security Service.**

1. Select **Policies > NAT**.
2. Click **Add**. The device displays the Security Policy Rule dialog.
3. On the **General** tab, **Name** the rule. For example, **no_nat**.
4. Add the source zone.
a. Click the **Original Packet** tab.

b. Add the **Source Zone** (the trust zone).

c. For the **Destination Zone**, select the zone you created in **Step 2**.

5. Disable NAT-T.

   a. Click the **Translated Packet** tab.

   b. From the **Translation Type** drop-down, select **None**.

6. Click **OK**.

**STEP 9—Create policy-based forwarding rules to route traffic over the IPSec tunnel.**

1. Select **Policies > Policy Based Forwarding**.

2. Click **Add**. The device displays the Security Policy Rule dialog.

3. On the **General** tab, **Name** the rule. For example, **WSS_OvertPsec_1**.

4. Add the source zone.
Firewall/VPN Access Method Guide: Palo Alto Site-to-Site VPN Configuration (PSK)/Page 93

a. Click the Source tab.

b. Add the Source Zone (the trust zone).

5. Add the destination services.

a. Click the Destination/Application/Service tab.

b. Add services.
For stand-alone IPSec deployments, click Add and select service-http and service-https; if you plan to configure the Web Security Service to perform SAML authentication over IPSec tunnels, select service-saml.

For trans-proxy deployments:
- All traffic directs to 199.19.250.205, which means only that address must be sent over the IPSec tunnel. Add it to the Destination Address area.
- In the Service area, add only service-http, which is port 80 traffic.

6. Configure the forwarding rule that sends traffic over the designated tunnel interface.

   ![Policy Based Forwarding Rule](image)

   a. Click the Forwarding tab.
   b. From the Action drop-down, select Forward.
   c. From the Egress Interface drop-down, select the tunnel created in Step 1.
   d. Assign the Monitor.
      i. Select Monitor.
      ii. Select the monitor profile created in Step 6.2.h.
      iii. Select **Disable this rule if nexthop/monitor IP is unreachable**. For more information about this option, see https://live.paloaltonetworks.com/docs/DOC-5952.
      iv. Enter the IKE Gateway IP Address (the Symantec datacenter IP).

7. Click OK.

8. For failover, clone this rule and configure it to forward traffic to the backup tunnel (if you created one in Step 1). Ensure that you change the monitor IP to the appropriate IKE Gateway IP address.

**STEP 10—Create a failover rule to discard traffic when both tunnels are down.**

For the final failover component, create a rule that discards traffic bound for the Web Security Service should both of the
IKE Gateway IP tunnels go down. Add this rule after that the rules that forward traffic to the service.

The final rules should look similar to the following.

![Rule Table]

**Next Selection**

- **Trans-Proxy deployment**: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.
- **Stand-alone IPsec deployment**: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Select a Firewall Device (Cert-Based)

You are here in the Firewall/VPN Access Method walkthrough.

The firewall performs a Simple Certificate Enrollment Protocol (SCEP) request to the Symantec partner (Entrust) to obtain the certificate used to authenticate itself to the service. This is a viable option if NAT-T is required in your environment.

Pre-Deployment: Select Authentication Method

Before configuring a firewall device to send traffic to the Web Security Service, Symantec recommends deploying a user authentication method. This is required for user reporting and pre-traffic policy creation.

If you have not completed this task, refer to the Authentication information in the Web Security Service Access Methods or Solutions WebGuides/PDFs.

Cert-based Configuration

Currently, Symantec has tested a cert-based configuration only on a Cisco device. You can attempt to configure other similar devices to perform a cert-based connection to the Web Security Service. As new devices are vetted, they are added to this official documentation.

Tip: You can search the Symantec Knowledge Base for your device in question. Occasionally, other subject matter experts upload procedures that were not officially tested.
Cert-Based IPsec Connection

The certificate-based IPsec connection to the Web Security Service provides an alternative to the VPN-to-VPN method that uses the mutual Preshare Key method to authenticate the Symantec Web Security Service. A common use case that requires the cert-based method is there are many firewalls behind the NAT firewall, which prevents the use of a unique gateway IP address.

Tip: For more conceptual information and use cases, see "About Certificate-Based Firewall Connections" on page 12.

Version Demonstrated:

- ASA 9.1 devices (ASDM 7.1(1)52).

Other devices that support Simple Certificate Enrollment Protocol (SCEP) might work, but Symantec cannot guarantee the results.

Deployment Notes

- Do not send Auth Connector traffic to the Web Security Service.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Procedure

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 firewall device and the Web Security Service.

1. In Service Mode, select **Account Maintenance > MDM, API Keys**.
2. If you do not already have an account to create Web Security Service APIs, create one.
a. In Service Mode, select **Account Maintenance > MDM, API Keys**.

![API Keys](image)

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 Web Security Service 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://portal.threatpulse.com/api/locations?name=location_name&type=cert-firewall`

   Where `location_name` is the name you assign. For example:

   `https://portal.threatpulse.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 Web Security Service generates the OTP. For example:

   ```json
   {"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 the firewall 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 Web Security Service revokes the previous certificate.

5. Verify that the Web Security Service created the new location. In **Service** mode, select **Network > Locations**.
Step 2—Import the root certificates (2048-bit) to your firewall device.

Symantec partners with Entrust to provide authentication certificates. You must import the 2048-bit certificate to your device.

1. Obtain the Entrust Certificate Authority—L1E certificate from Entrust.
   a. In a browser, navigate to: https://www.entrust.com/get-support/ssl-certificate-support/root-certificate-downloads/
   b. Locate the Root Certificate identified by the following:
      - **Serial Number**: 45 6b 50 54
      - **Thumbprint**: b3 1e b1 74 40 e3 6c 84 02 da dc 37 d4 4d 52 f9
   c. Click Download and open the file in a text editor.
2. In the ASDM interface, select **Configuration > Device Management, CA Certificates**.
3. Click **Add**. The device displays the Install Certificate dialog.
a. Name the Trustpoint. For example, **Entrust2048**.

b. Copy the certificate contents from the text file created in sub-step 1.c.

c. Select **Paste certificate in PEM format**: paste in the certificate contents.

d. Click **Install Certificate**.

e. Repeat this sub-step and paste in the contents of the **Entrust L1C Chain Certificate (SHA2)** certificate.

**Step 3—Create an Identity Certificate on the Firewall Device.**

Configure the device to perform a SCEP challenge and pair the identity certificate.

a. Name the Trustpoint as **BlueCoatIssuingCA**.

b. Select **Add a new identity certificate**.

c. You can accept the default **Key Pair**, but it must be 2048 bits.

d. Click **Advanced**. The device displays the Advanced Options dialog.

2. Enable the SCEP enrollment mode.

   a. Request by manual enrollment
   b. Request from a CA

   Enrollment URL (SCEP): http://bluecoatsweb.managed.entrust.com/scep
   
   Retry Period: 1 minutes
   
   Retry Count: 0 (Use 0 to indicate unlimited retries)
3. Set the SCEP challenge password.

   a. Click the **Enrollment** tab.
   
   b. Select **Request from a CA**.
   
   c. In the Enrollment URL (SCEP) field, enter:
      
      bluecoatasweb.managed.entrust.com/scep

4. Click **Install Certificate**.

**Step 4—Create the site-to-site VPN tunnel.**

Enable IKE access on the interface that will establish a VPN tunnel to the Web Security Service.
1. In the ASDM interface, click Configuration.
2. Click Site-to-Site VPN.
3. Click Connection Profiles.
4. In the Access Interfaces area, select Allow IKE v1 Access for the (outside) interface.
5. In the Connections Profile area, click Add; the device displays the Add IPsec Site-to-Site Connection Profile dialog.
a. Select the **Peer IP Address: Static** option and enter the regional Web Security Service primary IP address for this location (refer to your planning sheet). The **Connection Name** (selected by default) automatically fills in the same information.

b. For the **Protected Networks: Local Network** option, select the originating hosts or subnets that will send web traffic in this tunnel.

c. The **Protected Networks: Remote Network** setting depends on the Access Method:
   - For stand-alone deployments, select **any**.
   - For deployments, enter the SymantecWeb Security Service explicit proxy IP address: 199.19.250.205.

d. You can accept the default **Group Policy Name**, but verify that the **Enable IKE v2** option is cleared (the Web Security Service does not support v2).

e. Select the **Device Certificate** that you created in **Step 3**.

f. The **Encryption Algorithms: IKE Policy** option must contain an **rsa-sig** authentication.


h. From the left-menu, click **Crypto Map Entry**. The device displays the Edit IPsec Site-to-Site Connection Profile screen.
6. Define the Crypto Map and enable NAT-T.

![Crypto Map Configuration]

- **a.** Enable the **Perfect Forward Secrecy** option.
- **b.** Enable the **NAT-T** option.
- **c.** Select the **Device Certificate** that you created in **Step 3**.
- **d.** Click **OK**.

7. Click **OK** to close the Connection Profile dialog.

**Step 5—Create a backup peer.**

Enable IKE access on the interface that will establish a VPN tunnel to the Web Security Service.
1. In the ASDM interface, click **Configuration**.

2. Click **Site-to-Site VPN**.

3. Select **Advanced > Crypto Maps**.

4. Select the Crypto Map that you created in **Step 4** and click **Edit**. The device displays the Edit IPSec Rule dialog.
a. Enter a second Web Security Service data center IP address.

b. Click Add to move it to the peer list.

   At any time, you can return to this screen and use the Move Up and Down buttons to change the order.

c. Click OK.

**Step 6—Define NAT rules.**

Exclude web traffic on ports 80 and 443 from NAT.

1. On the ASDM interface, navigate to the **NAT Rules** page.
2. Click Add. The device displays the Add NAT Rule dialog.
Firewall/VPN Access Method Guide: Cert-Based IPsec Connection/Page 108

1. (Optional) Select a **Source Interface**.

2. For the **Source Address**, select the host or internal subnet.

3. (Optional) Select a **Destination Interface**.

4. From the **Destination Address** drop-down, select **any**.

5. From the **Service** drop-down, select **HTTP**.

   **Note:** If the HTTP and HTTPS service objects have not been created, you must do so in the ASDM interface.

6. Verify that the **Action: Translated packet / Source Address** option is **--Original--**.

7. Select the **Disable Proxy ARP on egress interface** option.

8. Click **OK**.

3. Repeat this step and create a NAT rule for the **HTTPS** service.
Next Selection

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.
- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Add Explicit Proxy Entry to PAC File (Trans-Proxy)

If you are configuring a trans-proxy solution (explicit proxy over IPsec), you must add an entry to your installed PAC file. This entry instructs all outbound web traffic (port 80) to exit the internal network through a firewall device (IPsec) and connect to the Symantec Web Security Service using the explicit proxy hostname.

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 configured proxy forwarding as your primary method but want to use trans-proxy to provide seamless back up to that. You ensure that traffic sent to proxy.threatpulse.net:8080 uses the firewall IPsec tunnel to the Web Security Service. The entry for this method is:
  
  ```
  return "PROXY corp-gw.mycompany.com:8080; PROXY ep.threatpulse.net:80";
  ```

- You have configured proxy forwarding as your primary method but want to use trans-proxy to provide seamless back up to that. You ensure that traffic sent to proxy.threatpulse.net:80 uses the firewall IPsec tunnel to the Web Security Service. 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 trans-proxy 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.pcs-computing.com") ||
        (host == "pcs-computing.com") ||
        (shExpMatch(host, ".pcs-intranet.com") ||
        (shExpMatch(host, "90.0.0.*")) ||
        (shExpMatch(host, "10.*")) {
        return "DIRECT"
    } else {
    return "PROXY ep.threatpulse.net:80"
    }
}
```

Next Step

Proceed to "Verify Service Connectivity to Locations" on page 171.
If you have an older model, Symantec previously provided device-specific procedures. These are now provided as legacy.

- "Check Point (Simplified Mode): Create Site-to-Site VPN Connection" on page 112
- "Cisco 1941: Create a Site-to-Site VPN Connection" on page 126
- "Cisco ASA (Pre 8.3): Create a Site-to-Site VPN Connection" on page 130
- "Cisco ASA (8.3/8.4): Create a Site-to-Site VPN Connection" on page 141
- "Fortinet: Create a Site-to-Site VPN Connection" on page 153
- "Juniper SSG20: Create a Site-to-Site VPN Connection" on page 160
Check Point (Simplified Mode): Create Site-to-Site VPN Connection

The most basic concept for this method is configure the router with a site-to-site domain-based VPN connection. The site comprises the gateway and the encryption domain. Defined device policy rules then send web-based traffic to the Web Security Service and ignore everything else. This procedure provides basic configuration steps for Simplified Mode. It is likely that you have an existing Check Point device configured in your network; therefore, slight alterations to the existing deployment might be required. For failover, you must create two VPN gateways.

Deployment Notes

- These procedures assume that you are already logged into the Check Point Smart Dashboard interface. The configuration tasks in this topic demonstrate with the following versions.
  - Check Point Gateway running R77.30.
  - Security Manager running R77.30.
  - SmartConsole R77.30.
  - EndPoint Security test with E80.50(8.3.937).

If you are using another version, options might vary.

Note: R77.20 is the minimum supported version because of the Dead Peer Dead requirement.

- NAT-T cannot be enabled on the router/firewall device. The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Procedure

Prerequisite—Verify that the device is ready for configuration.

This procedure assumes that the Check Point device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

Step 1—Create Symantec Encryption Domain.

Create a Simple Group of the five IP Address Ranges that define all Internet addresses. These ranges include loopback, RFC1918, and Class D and E.
1. In the SmartDashboard, select **Network Objects**.

2. Right-click **Address Ranges** and select **Address Ranges > Address Range**.

![Network Objects]

The interface displays the Address Range Properties dialog.

3. Define the first Internet range.

![Address Range Properties - internet_range1]

- **Name** the range.
- **First IP address** field, enter **1.0.0.0**.
  
  **ALTERNATIVE:** If you are configuring a Trans-Proxy deployment (Explicit over IPsec), enter **199.19.250.205** and proceed to sub-step 5.

- **Last IP address** field, enter **9.255.255.255**.
- Click **OK**.

4. Repeat **Step 1.3** (above) four times to complete the Internet ranges.
a. **First IP address**: 11.0.0.0; **Last IP address**: 126.255.255.255.
b. **First IP address**: 128.0.0.0; **Last IP address**: 172.15.255.255.
c. **First IP address**: 172.32.0.0; **Last IP address**: 192.167.255.255.
d. **First IP address**: 192.169.0.0; **Last IP address**: 223.255.255.255.

5. Create the Simple Group. Remaining in the **Network Objects** applet, right-click **Groups** and select **Simple Group**. The interface displays the Group Properties dialog.

   a. **Name** the group.
   b. From the **Not in Group** area, select the five range objects that you created in **Steps 1.3 and 1.4**.
   c. Click **Add** to move them **In Group**.
   d. Click **OK**.

**Step 2—Create the Local Encryption Domain.**

When a location is active, all outbound port 80 and 443 web traffic routes through the VPN tunnel to the Web Security Service. The following example identifies the subnets that you want sent to the service for processing.

**Tip:** Symantec assumes that this is an existing gateway device and that you have previously configured to send traffic to the Internet. If you do not have subnets configured, consult the documentation for the Check Point device.
1. In the **Network Objects** applet, right-click **Groups** and select **Simple Group**. The interface displays the Group Properties dialog.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue_Coat_Encryption_Domain</td>
<td>198.135.12...</td>
</tr>
<tr>
<td>BlueC...</td>
<td>196.156.12...</td>
</tr>
<tr>
<td>CP_defa...</td>
<td>172.16.0.0...</td>
</tr>
<tr>
<td>CPDS...</td>
<td>193.16.16.12...</td>
</tr>
<tr>
<td>DMZNet</td>
<td>192.168.1.0...</td>
</tr>
<tr>
<td>DMZNet</td>
<td>192.168.1.0...</td>
</tr>
</tbody>
</table>
```

a. **Name** the group.

b. From the **Not in Group** area, select internal subnets that transport Internet-bound traffic.

c. Click **Add** to move them **In Group**.

d. Click **OK**.

**Tip:** To perform Web Security Service testing, you can identify a single workstation to send rather than entire production subnets. When you are satisfied, edit the object to add the production subnets.

---

**Step 3—Exclude Non-Web Traffic (Protocol Ports)**

Create an protocol group that excludes the non-web protocols from inclusion in the VPN tunnel that connects to the Web Security Service.
1. In the SmartDashboard, select **Services**.

2. Right-click **Group** and select **New Group**. The interface displays the Group Properties dialog.

3. Click **New**. The interface displays the Group Properties dialog.
   a. **Name** the object. For example, indicate that these are ports 1 to 79.
   b. In **Port** field, enter **1-79**. This excludes all ports up to 80 (web).
   c. Click **Advanced**. The interface displays the Advanced TCP Service Properties dialog.
   d. Select **Match For 'Any'**. This prevents policy installation warnings because of a possible already-defined port.
   e. Click **OK**; click OK again to close the Group Properties dialog.

4. Repeat **Steps 3.1** through **3.3** to add two more groups.
   a. Mid-TCP-Ports: **81 to 442**.
   b. High-TCP-Ports: **444 to 65535**.

   This allows port 443 traffic into the VPN tunnel.

5. (Optional) You can also add ICMP and all UDP ports.

**Step 4—Define the Gateway.**

Create a Gateway (Interoperable Device) that points to the nearest Symantec datacenter for the configured location. Refer to your **planning sheet** for the datacenter IP address.
1. In the SmartDashboard, select **IPSec VPN** from the top ribbon.
2. From the left-menu, select **Gateways**.
3. From the **Gateway** options, click **+Add**. The interface displays the Interoperable Device dialog.
   a. **Name** the gateway.
   b. Enter the Web Security Service **IPv4 Address**.
   c. Click **OK**.
4. Add the Symantec Encryption Domain.
   a. **Edit** the new gateway.
   b. From the left-menu, select **Topology**.
   c. In the **VPN Domain** area, select **Manually Defined**.
   d. Click the browse icon-button (...) and select the Encryption Domain that you configured in **Step 1**.
   e. Click **OK**.
5. Add the Encryption Domain to Check Point gateway.
   a. From the left-menu, select **Gateways**.
   b. Select the configured Check Point gateway and click **Edit**. The interface displays the Check Point Gateway dialog.
   c. Select **Topology**.
d. Select the **External** interface.

e. In the **VPN Domain** area, select **Manually Defined**.

f. Click the browse icon-button (…) and select the Local Encryption Domain that you configured in **Step 1**.

g. Click **OK**.

**Step 5—Create the VPN Community**

Add the Check Point gateway and the Symantec device to participating gateways.

1. In the SmartDashboard, select **IPSec VPN** from the top ribbon.

2. From the left-menu, select **Communities**.

3. From the **Communities** options, select **New > Meshed Community**. The interface displays the Meshed Community Properties dialog.

   a. **Name** the community.

   b. Select **Participating Gateways**.
c. Click **Add**. The interface displays the Add Participating Gateways dialog.

d. The interface detects the available gateways. Select the Check Point gateway and the Web Security Service gateway that you created; click **OK**.

e. From the left-menu in the dialog, select **Tunnel Management**.

f. Select **One VPN tunnel per Gateway pair**.

g. From the left-menu in the dialog, select **Advanced Settings > Excluded Service**.
Firewall/VPN Access Method Guide: Check Point (Simplified Mode): Create Site-to-Site VPN Connection/Page 120

4. Establish the pre-shared key (PSK). Remaining under Advanced Settings, select Shared Secret.

- Click Add.
- In the Add Service dialog, scroll to and select the Excluded Protocols object that you created in Step 3.
- Click OK.
a. The dialog contains the Web Security Service peer that you configured. Select it and click **Edit**.

b. Enter the pre-shared key (**Secret**) used to by the Web Security Service to authenticate the tunnel and click **Set**. Refer to your planning sheet.

Tip: The PSK must be at least eight characters and **cannot** use special characters.

c. Click **OK**.

5. Select the Internet Key Exchange algorithm and disable NAT-T. Remaining under **Advanced Settings**, select **Advanced VPN Properties**.


b. Verify that **Disable NAT inside the VPN community** is selected.

**Step 6—Configure Check Point Gateway for Dead-Peer-Dead.**

Change the tunnel keep-alive method to Dead-Peer-Dead (DPD).
1. Log in to GuiDBedit, the Check Point database tool.

   
   a. Select **Table > Network Objects > network_objects**.
   
   b. Select the Check Point gateway device.
   
   c. In the **Field Name** column, scroll down to **VPN > tunnel_keepalive_method**.
   
   d. Right-click **Value** and select **Edit**; in the dialog, select **dpd**.
   
   e. Click **OK**.

2. Repeat Step 1.1 for each configured Symantec gateway.

3. Click **Save All Changed Objects** (upper-left corner).

4. Return to the SmartDashboard and click **Install Policy**.

**Step 6—Enable Dead-Peer-Dead.**

To avoid datacenter connection issues, you must enable Dead-Peer-Dead on the Check Point device. You cannot accomplish this through the SmartDashboard. You must use the Check Point Database Tool (GuiDBedit).

1. Access the GuiDBedit program, which is located in the SmartConsole **PROGRAM** folder.

   a. For example, on Windows, the default path to navigate to is:

   `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.30\PROGRAM`

   b. Run the GuiDBedit program.

2. In the database tool, set Dead Peer Dead only on the Web Security Service gateway object(s).
In the Tables tab, select Network Objects > Network Objects.

b. Scroll through Object Names to locate the Web Security Service gateway object that you created.

c. Scroll through the Field Names to locate tunnel_keepalive_method.

d. Double-click dpd and enable it.

e. Save the database tool changes.

3. Return to the SmartDashBoard and Install the policy.

Step 7—Exclude Auth Connector Traffic from the Web Security Service.

If Auth Connector traffic requires access to the Internet through the Check Point gateway, you must exclude that traffic from routing to the Web Security Service. Many datacenters have several to many Auth IP addresses. This step describes how exclude subnets verses manually configuring individual addresses.

Tip: If your Access Method is Trans-Proxy (IPsec over VPN), you can skip this step.

1. In the SmartDashboard, select Network Objects.

2. Right-click Networks and select Network.
3. Define the first Internet range.

   a. **Name** the property; for example, indicate that these addresses are for authentication traffic.

   b. In the **Network Address** field, enter the IP address range for the datacenter to which this location sends traffic. For example, several of the Auth Connector addresses for the Chicago, USA datacenter reside in 198.135.124.xxx. Therefore, enter **198.135.124.128**.

       **Tip:** For a list of authentication addresses per datacenter, see "Reference: Authentication IP Addresses" on page 26.

   c. In the **Net Mask** field, enter the calculated subnet mask address. This instructs the object to include all addresses in this range.

   d. Click **OK**.

4. Add this object to the Excluded Domains object that you created in **Step 2**.
Next Selection

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.

- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Cisco 1941: Create a Site-to-Site VPN Connection

The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways. This procedure provides basic configuration steps for a single device. It is likely that you have an existing 1941 device configured in your network; therefore, slight alterations to the existing deployment might be required.

Deployment Notes

- This configuration task uses the Classic Mode, Web Security Service. You must use the Cisco IOS CLI interface to complete this task. The following command output only provides elements relevant to the Web Security Service VPN-to-VPN configuration, not the entire device configuration relevant to your gateway deployment.
- NAT-T cannot be enabled on the router/firewall device. The Web Security Service does not support that configuration at this time. The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.
- There are two sets of base VPN configurations: one for stand-alone Firewall/VPN Access Method and one for the Trans-Proxy Access Method.
- These procedures assume that you are already logged into the Cisco IOS Interface.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Tip: italic_font = variable for user input

Base VPN Configuration - Firewall/VPN Access Method

crypto isakmp policy 1
encr aes
authentication pre-share
group 5
crypto isakmp key 12345678 address wss_primary_IP_address
crypto isakmp keepalive 10 periodic
crypto isakmp aggressive-mode disable
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
crypto map outside_map 1 set nat-t-disable
!
For IOS release 12.2(13)T and later, use: no crypto ipsec nat-transparency udp-encaps
crypto map SDM_CMAP_1 1 ipsec-isakmp
set peer wss_primary_IP_address
set transform-set ESP-AES-SHA
set pfs group5
match address IPSEC_TRAFFIC
!
interface FastEthernet0/0
ip address outside_IP_address {mask}
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet0/1
ip address inside_IP_address {mask}
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
!
ip default-gateway gateway_IP_address
!
ip nat inside source list nat_rule interface FastEthernet 0/0 overload
!
ip access-list extended IPSEC_TRAFFIC
permit tcp InternalNetworkFirewall_IP {mask} any eq www
permit tcp InternalNetworkFirewall_IP {mask} any eq 443
ip access-list extended nat_rule
deny tcp InternalNetworkFirewall_IP {mask} any eq www
deny tcp InternalNetworkFirewall_IP {mask} any eq 443
permit ip InternalNetworkFirewall_IP {mask} any
Base VPN Configuration - Trans-Proxy Access Method

crypto isakmp policy 1
encr aes
authentication pre-share
group 5
crypto isakmp key 12345678 address wss_primary_IP_address
crypto isakmp keepalive 10 periodic
crypto isakmp aggressive-mode disable
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
crypto map outside_map 1 set nat-t-disable
!
For IOS release 12.2(13)T and later, use: no crypto ipsec nat-transparency udp-encaps
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
set peer wss_primary_IP_address
set transform-set ESP-AES-SHA
set pfs group5
match address IPSEC_TRAFFIC
!
interface FastEthernet0/0
ip address outside_IP_address {mask}
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet0/1
ip address inside_IP_address {mask}
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
!
ip default-gateway gateway_IP_address
!
ip nat inside source list nat_rule interface FastEthernet 0/0 overload
!
ip access-list extended IPSEC_TRAFFIC
permit tcp InternalNetworkFirewall_IP {mask} 199.250.205 eq www
ip access-list extended nat_rule
deny tcp InternalNetworkFirewall_IP {mask} any eq www
permit ip InternalNetworkFirewall_IP {mask} 199.250.205

**Failover Config**

After the Crypto Map is set up for a single tunnel, perform the following steps to configure failover peers:

1. Each failover peer has to be added to crypto map:

   ```
   set peer wss_backup_ip_address
   ```

2. Configure the PSK for each of the peers (same PSK is used on all datapods):

   ```
   crypto isakmp key aaaabbbbcddddd address 1.0.0.110
   ```

   **Tip:** The PSK must be at least eight characters and cannot use special characters.

3. Configure keepalive behavior:

   ```
   "crypto isakmp keepalive keepalive_interval keepalive_fail_interval {on-demand | periodic}"
   ```
   - The `keepalive_interval` is the interval between subsequent keepalives. The minimum is 10 seconds.
   - The `keepalive_fail_interval` is the interval between keepalive messages after a keepalive failure. The minimum (and default) value is 2.
   - The `{on-demand | periodic}` option—If `periodic` is set, the device will send a keepalive every interval. If `on-demand` (the default) is set, keepalives are sent only when some traffic is flowing through the tunnel.

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.
- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Cisco ASA (Pre 8.3): Create a Site-to-Site VPN Connection

The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways. This procedure provides basic configuration steps. It is likely that you have an existing ASA device configured in your network; therefore, slight alterations to the existing deployment might be required.

**Tip:** Symantec recommends the ASA v8.3 or later devices (running ASDM 6.4 or later). These versions allow for simplified, less intrusive policy changes on the devices than pre-8.3 devices.

**Deployment Notes**

- These procedures assume that you are already logged into the Cisco ASDM Web Interface. The configuration tasks in this topic use ASDM v6.2. If you are using another version, options might vary.
- NAT-T cannot be enabled on the router/firewall device. The Web Security Service does not support that configuration at this time. The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.

**Note:** Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. *The screenshots in the following procedure might not reflect this advisory.*

**Procedure**

**Prerequisite—Verify that the router is ready for configuration.**

This procedure assumes that the Cisco ASA device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

1. Select the **Configuration > Interfaces > Switch Ports** tab.
2. Verify the list has one interface is required for the outside (Web Security Service) connection and as many available interfaces for inside routes (see planning sheet).

**Step 1—Create a site-to-site connection profile.**

1. Access the Connection Profile dialog.
a. Select **Configuration**.

b. Click **Site-to-Site VPN**.

c. In the **Connection Profiles** area, click **Add**. The device displays the Add IPsec Site-to-Site Connection Profile dialog.

2. Configure the IPsec site-to-site connection profile.
a. Select the **Peer IP Address:** Static option and enter the regional Web Security Service primary IP address for this location (refer to your planning sheet). The **Connection Name** (selected by default) automatically fills in the same information.

b. For the **Interface** option, select outside.

c. Enter the **Pre-shared Key,** which is the string used to secure the encrypted tunnel between the router and the Web Security Service (eight-character minimum; refer to your planning sheet).

**Tip:** The PSK must be at least eight characters and cannot use special characters.

d. For the **Protected Networks:** Local Network option, select inside-network.

e. For the **Protected Networks:** Remote Network option, select any.

f. The **Protected Networks:** Remote Network setting depends on the Access Method:

   - For stand-alone IPsec deployments, select any.
   - For trans-proxy deployments, enter the Symantec Web Security Service explicit proxy IP address: 199.19.250.205.

g. Remain in the IPsec Site-to-Site Connection Profile dialog and proceed to **Step 3**.

3. Create and/or select supported encryption/authentication protocols. The Cisco ASA device-to-Web Security Service access method requires selecting a supported **IPsec Proposal.** Cisco references groups of these as *transform sets.* The Web Security Service supports many combinations. See "Reference: IKE Encryption and Authentication Algorithms" on page 27.
To display the Select Transform Set dialog, click Select (next to the IPsec Proposal field).

4. In the IKE Proposals area, verify that the options are 3DES or AES. Click Manage and delete others. Click OK.
5. Remain in the Connection Profile dialog and select Advanced > Crypto Map entry.
Firewall/VPN Access Method Guide: Cisco ASA (Pre 8.3): Create a Site-to-Site VPN Connection/Page 134

Step 1—Create the IPsec Site-to-Site Connection Profile:

1. In the Configuration > Site-to-Site VPN module, select Advanced > IPsec Profiles.
2. Click Add.
3. Define the IPsec Site-to-Site Connection Profile as follows:
   - Priority: 1
   - Perfect Forward Secrecy: Enable
   - Diffie-Hellman Group: group5
   - NAT-T: Enable
   - Reverse Route Injection: Enable
   - Security Association Lifetime:
     - Time: 86400
     - Traffic Volume: 4608000

   a. Enable the Perfect Forward Secrecy option.
   b. For the Diffie-Hellman Group option, select group5.
   c. Clear the NAT-T option.
   d. Click OK to close the dialog.

Step 2—Create the IPsec connection rule for HTTP and HTTPS traffic.

1. In the Configuration > Site-to-Site VPN module, select Advanced > Crypto Maps.
2. Click Add.
3. Define the Tunnel Policy (Crypto Map) - Basic tab options as follows.
a. Set the **Priority** for this policy; the highest priority overrides other policies that have matching values. You cannot assign the same priority as another policy; modify this one or the other.

b. Select a supported **Transform Set**. Symantec recommends **PRE-G5-AES128-SHA**. See **Prerequisite B** above.

c. For **Connection Type**, select **bidirectional**.

d. **IP Address of Peer to Be Added**—Enter your regional Web Security Service IP address (refer to your planning sheet) and backup address if your region requires it; click **Add**.

e. Select **Enable Perfect Forwarding Secrecy** and for **Diffie-Hellman Group**, select **group5** (1536 bits).

4. Click the **Traffic Selection** tab and configure the options as follows.
Step 3—Enable the IKE parameters.

1. Select Configuration > Advanced > IKE Parameters.
2. Enable the inside interface and verify NAT is disabled.
   
   a. In the Enable IKE area, select the inside interface and click Enable.
   
   b. Clear the Enable IPsec over NAT option.
3. Click Apply.

Step 4—Define connection profile map policy.
1. Select Configuration > Advanced > Certificate to Connection Profile Maps > Policy.

2. Select every option except the first one: Use the configured rules to match a certificate to a Connection Profile.
   
3. Click Apply.

Step 5—Bypass interface access lists.

1. Select Configuration > Advanced > System Options.

2. Select the first option: Enable inbound IPsec sessions to bypass interface access lists.

3. Clear the other options.

4. Click Apply.
Step 6—Create a NAT rule.

1. Select Configuration > Firewall > NAT Rules.

2. You must delete any existing default dynamic NAT rules. Also, port 80 and 443 must not be a part of any NAT rule because NAT rules apply before the Crypto Map rules.

3. Click Add and select Dynamic Policy NAT Rule.

4. Continuing with the dynamic policy NAT rule, define the type of NAT rule used. In the Translated area select the outside Interface/outside Address Pool rule and click Manage.
a. Select the **outside Interface/outside Address Pool** from the Pool list and click **Edit**. The Edit Global Address Pool dialog displays.

b. Select the **Port Address Translation (PAT) using IP Address of the Interface** option and click **OK**.

5. Click **OK** to close the Manage Global Pool dialog.

6. Click **OK** to add the NAT policy.

7. At the bottom of the **NAT Rules** page, select the **Enable traffic through the firewall without address translation** option.

8. Repeat Steps 3 through 6 to add `<tcp/80` and `tcp/443` rules.

9. Repeat to add other protocols, such as UDP.
10. You must delete any existing NAT policies that include subnets to be forwarded to the Web Security Service; they are not compatible with the required policy.

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.

- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Cisco ASA (8.3/8.4): Create a Site-to-Site VPN Connection

The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways. You can designate host or subnet that tests the IPsec connectivity to the Web Security Service without interrupting the production traffic. After successful testing, add production subnets.

This procedure provides basic configuration steps. It is likely that you have an existing ASA device configured in your network; therefore, slight alterations to the existing deployment might be required.

Deployment Notes

- NAT-T cannot be enabled on the router/firewall device. The Web Security Service does not support that configuration at this time. The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.

Note: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The screenshots in the following procedure might not reflect this advisory.

Procedure

Prerequisite—Verify that the router is ready for configuration.

This procedure assumes that the Cisco ASA device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

1. Select the Configuration > Interfaces > Switch Ports tab.
2. Verify the list has one interface is required for the outside (Web Security Service) connection and as many available interfaces for inside routes (see planning sheet).

Step 1—Create a site-to-site connection profile.

1. Access the Connection Profile dialog.
a. Select **Configuration**.

b. Click **Site-to-Site VPN**.

c. In the **Connection Profiles** area, click **Add**. The device displays the Add IPsec Site-to-Site Connection Profile dialog.

2. Configure the IPsec site-to-site connection profile.
a. Select the Peer IP Address: Static option and enter the regional Web Security Service primary IP address for this location (refer to your planning sheet). The Connection Name (selected by default) automatically fills in the same information.

b. For the Interface option, select outside.

c. Enter the Pre-shared Key, which is the string used to secure the encrypted tunnel between the router and the Web Security Service (eight-character minimum; refer to your planning sheet).

Tip: The PSK must be at least eight characters and cannot use special characters.

d. For the Protected Networks: Local Network option, select inside-network.

e. The Protected Networks: Remote Network setting depends on the Access Method:
   - For stand-alone IPsec deployments, select any.
   - For Trans-Proxy deployments, refer to “About Trans-Proxy (Explicit Proxy Over IPsec)” on page 20 for options.

f. Remain in the IPsec Site-to-Site Connection Profile dialog and proceed to Step 3.


To display the Select Transform Set dialog, click Select (next to the IPsec Proposal field).
a. Click Add. The Add Transform Set dialog displays.

b. Name the proposal.

c. For the Tunnel option, select Mode.

d. For the ESP Encryption option, select a supported encryption type (Symantec recommends AES128).

e. Select an ESP Authentication option (Symantec recommends SHA).

f. Click OK to close the Add dialog.

g. In the Assigned IPsec Proposals area, clear all listed proposals and select and Assign the proposal that you just created.

h. Click OK to close the Transform Sets dialog.

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

5. Remain in the Connection Profile dialog and select Advanced > Crypto Map entry.
6. Click **OK** to close the Connection Profile dialog.

7. Repeat this task to create a VPN for the additional Web Security Service IP addresses (see your planning sheet).

**Step 2—Create the IPsec connection rule for HTTP and HTTPS traffic.**

1. Still in the **Configuration > Site-to-Site VPN** module, select **Advanced > Crypto Maps**.
2. Click **Add**.
3. Define the **Tunnel Policy (Crypto Map) - Basic** tab options as follows.
a. Set the **Priority** for this policy; the highest priority overrides other policies that have matching values. You cannot assign the same priority as another policy; modify this one or the other.

b. Select a supported **Transform Set**. See “Reference: IKE Encryption and Authentication Algorithms” on page 27.

c. For **Connection Type**, select **bidirectional**.

d. **IP Address of Peer to Be Added**—Enter your regional Web Security Service IP address (refer to your
planning sheet) and backup address if your region requires it; click Add.

e. Select Enable Perfect Forwarding Secrecy and a supported Diffie-Hellman Group value.

4. Click the Traffic Selection tab and configure the options as follows.

<table>
<thead>
<tr>
<th>Create IPsec Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic Selection</strong></td>
</tr>
<tr>
<td>Action: <strong>Protect</strong></td>
</tr>
<tr>
<td>Source: inside-network/24</td>
</tr>
<tr>
<td>Destination: any</td>
</tr>
<tr>
<td>Service: tcp/http, tcp/https</td>
</tr>
</tbody>
</table>

a. For Action, select Protect.

b. Select the Source object designated as the inside network (interfaces to be routed to the Web Security Service).

c. For Destination, select Any.

d. For Service, select http and https.

5. Click OK to add the IPsec rule.

**Step 3—Enable the IKE parameters.**

1. Select Configuration > Advanced > IKE Parameters.

2. Enable the inside interface and verify NAT is disabled.
a. In the Enable IKE area, select the inside interface and click Enable.

b. Clear the Enable IPsec over NAT option.

3. Click Apply.

**Step 4—Define connection profile map policy.**

1. Select **Configuration > Advanced > Certificate to Connection Profile Maps > Policy.**

   ![Certificate to Connection Profile Map](image)

2. Select every option except the first one: **Use the configured rules to match a certificate to a Connection Profile.**

3. Click **Apply.**

**Step 5—Bypass interface access lists.**

1. Select **Configuration > Advanced > System Options.**
2. Select the first option: **Enable inbound IPsec sessions to bypass interface access lists**....
3. Clear the other options.
4. Click **Apply**.

**Step 6.8-3**—Follow this step if your ASA is a v8.3 device. Create NAT rules for Web Security Service-bound traffic.

1. Select **Configuration > Firewall > NAT Rules**.
2. Click **Add** and select **Add NAT Rule Before “Network Object” NAT Rules**.

3. The device displays the **Add NAT Rule dialog**. Configure the rule to route HTTP traffic from the inside network to the network egress (cloud service).
a. For **Source Interface**, select **inside** (the internal network traffic source object).

b. For **Destination Interface**, select **outside** (the network egress interface object).

c. For **Source Address**, select a single workstation object or a test subnet object for which you want to test cloud service connectivity. This host must be able to resolve DNS from a local DNS server.

d. For **Destination Address**, select a **Any**.

e. For **Service**, select a **HTTP**.

f. Select the **Disable Proxy ARP on egress interface** option. This option disables direction and assumes unidirectional.

g. Click **OK**.

4. Repeat **Step 6.8-3.3** and create a NAT rule for the **HTTPS** service; select the same source and destination values.

**Step 6.8-4**—Follow this step if your ASA is a v8.4 or later device. Create NAT rules for Web Security Service-bound traffic.

1. Select **Configuration > Firewall > NAT Rules**.

2. Click **Add** and select **Add NAT Rule Before "Network Object" NAT Rules**.
3. The device displays the Add NAT Rule dialog. Configure the rule to route HTTP traffic from the inside network to the network egress (cloud service).

- a. For **Source Interface**, select *inside* (the internal network traffic source object).
- b. For **Destination Interface**, select *outside* (the network egress interface object).
- c. For **Source Address**, select a single workstation object or a test subnet object for which you want to test cloud service connectivity. This host must be able to resolve DNS from a local DNS server.
d. For **Destination Address**, select a **Any**.
e. For **Service**, select a **HTTP**.
f. For **Direction**, select **Unidirectional**.
g. Click **OK**.

4. Repeat **Step 6.8-4.3** and create a NAT rule for the HTTPS service; select the same source and destination values.

### Step 7—Verify Traffic and Add Other Sources

The NAT rules indicate what internal sources are directed to the Web Security Service.

![Configuration > Firewall > NAT Rules](image)

This example exempts HTTP and HTTPS requests sent from **workstation1** (the test client) from Network Address Translation (NAT) by the device.

Generate some Web traffic from workstation1. Log in to the Web Security Service and check reports for requests by the test client. See “Verify Service Connectivity to Locations” on page 171.

When you are satisfied that the Web Security Service is receiving and processing data from this deployment, return to **Steps 6.8-3 or 6.8-4** and add more subnets to the **Source Address** in sub-step 3 (if necessary, create objects that contain the applicable clients/subnets).

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.
- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Fortinet: Create a Site-to-Site VPN Connection

The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways. This procedure provides basic configuration steps. It is likely that you have an existing Fortinet device configured in your network; therefore, slight alterations to the existing deployment might be required.

This procedure provides basic configuration steps for a route-based method, which provides tunnel redundancy. The procedure demonstrates with a Fortigate 300C, v4.0,build 4227,120816 (MR3). Symantec also tested on Fortigate 80CM running firmware v4.0, build 0521,120313 (MR3 Patch 6). If you are using another version, options might vary.

Deployment Notes

- These procedures assume that you are already logged into the Fortinet interface.
- NAT-T cannot be enabled on the router/firewall device. The Web Security Service does not support that configuration at this time. The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.

**Note:** Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. *The screenshots in the following procedure might not reflect this advisory.*

Procedure

Prerequisite—Verify that the device is ready for configuration.

This procedure assumes that the Fortinet device is already configured with the inside interface or group object with multiple inside interfaces and an outside interface that will communicate with the Web Security Service.

STEP 1—Create Phase 1 for primary tunnel.

1. From the left-menu, select **VPN > IPsec > Auto Key (IKE)**.
2. Click **Create Phase 1**.
3. The interface displays the **New Phase 1** screen. Define the Phase 1 tunnel.
a. Enter a meaningful **Name** for the tunnel interface. For example, the location of the device.

b. The **Remote Gateway** must be a **Static IP Address**.

c. From your **planning sheet**, enter the Web Security Service **IP Address**.

**TRANS-PROXY ALTERNATIVE:**

- For Trans-Proxy deployments, refer to "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20 for options; then proceed to sub-step 5.

d. Select the **Local Interface** from which the device initiates the tunnel connection to the Web Security Service (outside interface).

e. Enter the **Pre-shared Key**, which is the string used to secure the encrypted tunnel between the router and the Web Security Service (eight-character minimum; refer to your planning sheet).

**Tip:** The PSK must be at least eight characters and **cannot** use special characters.

f. Click **Advanced** to display more options.
g. Select Enable IPsec Interface Mode. The default IKE Version: 1 and Local Gateway IP: Main Interface IP settings are acceptable.

h. For the P1 Proposal, the Web Security Service supports many combinations. See "Reference: IKE Encryption and Authentication Algorithms" on page 27.

i. Clear the NAT Traversal option.

j. Select the Dead Peer Detection option.

k. Click OK.

**STEP 2—Create the Phase 2 for the primary tunnel.**

1. Click Create Phase 2.

2. The interface displays the New Phase 2 screen. Define the Phase 2 tunnel.

   - **Name**: 
     - Enter a Name that is similar to Phase 1. For example, nameP2.

   - **Phase 1**: 
     - From the Phase 1 drop-down, select the Phase 1 configuration that you created in Step 1. If you click Advanced, the interface displays the configurations that the Phase 2 inherits.

   - **P2 Proposal**: 
     - Encryption: 3DES Authentication: SHA1
     - Encryption: AES128 Authentication: SHA1
     - Enable replay detection
     - Enable perfect forward secrecy (PFS)
     - DH Group: 1 2 5 14
     - Keylife: Seconds 1800 (Seconds) 4508000 (KBytes)

   - **Autokey Keep Alive**: 
     - Enable

3. Click OK.

**STEP 3—Create secondary tunnel.**

Repeat Steps 1 and 2 to create the tunnel configuration for the secondary, or back-up, tunnel.

When complete, the Interface Modes should be similar to the following screen.
STEP 4—Create static routes.

Static routes are required to route web traffic over the VPN tunnel interfaces. To ensure that these routes are evaluated without risk to currently configured static routes, set the priorities higher.

1. From the left-menu, select **Router > Static > Static Route**.
2. Click **Create New**.
3. Create the static route for the primary tunnel that you created in **Step 1**.
   - a. From the **Device** drop-down, select the primary tunnel.
   - b. Click **Advanced**.
   - c. Assign the route a high **Priority** value.
   - d. Click **OK**.
4. Repeat **Steps 4-2** and **4-3** to create a static route for the secondary tunnel. Assign the **Priority** as slightly higher than the primary tunnel.

STEP 5—Create policy routes.

You must create policy that routes HTTP and HTTPS only traffic to the default routes for each VPN tunnel interface.

1. In the left-menu, select **Router > Static > Policy Route**.
2. Click **Create New**. The interface displays the **New Routing Policy** screen.
3. Define policy that routes HTTP (port 80) traffic from the inside interface to the outgoing interface.

   ![New Routing Policy](image)

   a. Set the **Protocol** to 6 (for TCP).

   b. From the **Incoming Interface** drop-down list, select the inside interface, or the interface that receives web-bound traffic.

   c. As this policy route is for HTTP traffic, set both the **Destination Ports** to 80 (both From and To).

   d. From the **Outgoing Interface** drop-down list, select the primary tunnel that you created in **Step 1**.

4. Click **OK**.

5. Repeat **Steps 5-2** and **5-3** to create a policy route for HTTPS traffic. Enter 443 in the **Destination Ports From** and **To** fields.

6. Repeat **Steps 5-2** and **5-3** to create HTTP and HTTPS policy routes for the secondary tunnel.

**STEP 6—Create firewall policies.**

You must create two rules to allow HTTP and HTTPS traffic through the VPN interfaces.

1. In the left-menu, select **Policy > Policy > Policy**.

2. Click **Create New**. The interface displays the **New Policy** screen.

3. Define policy that allows HTTP and HTTPS traffic through the primary tunnel interface to the Web Security Service.
Firewall/VPN Access Method Guide: Fortinet: Create a Site-to-Site VPN Connection/Page 158

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>a</th>
<th>port2 (INSIDE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>b</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>c</td>
<td>BCloudSvale</td>
</tr>
<tr>
<td>Destination Address</td>
<td>d</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>e</td>
<td>HTTP / HTTPS</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

a. From the **Source/Interface** drop-down list, select the inside interface, or the interface that receives Web-bound traffic.

b. From the **Source Address** drop-down list, select **all**.

   **TEST OPTION:** If you have specified a test client object in your Fortinet device, you can select that IP address here. When you are satisfied with the test results, you can return here and change to **all**.

c. From the **Destination Interface/Zone** drop-down list, select the primary tunnel interface that you created in **Step 1**.

d. From the **Destination Address** drop-down list, select **all**.

e. From the **Service** drop-down list, select **HTTP**; click the plus (+) icon and select **HTTPS**.

f. Click **OK**.

4. Repeat Steps 6-2 and 6-3 to create the policy for the secondary tunnel.

   The interface displays the new inside-to-VPN tunnel policy rules.

5. To ensure security, create a third rule on the internal WAN interface that denies HTTP and HTTPS traffic. If you do not create this rule, the WAN interface allows unchecked Web traffic. If this result is acceptable, you can skip this step.
a. Click **Create New**. The interface displays the **New Policy** screen.

b. From the **Source/Interface** drop-down list, select the inside interface, or the interface that receives Web-bound traffic.

c. From the **Source Address** drop-down list, select **all**.

d. From the **Destination Interface/Zone** drop-down list, select the default outside interface.

e. From the **Destination Address** drop-down list, select **all**.

f. From the **Service** drop-down list, select **HTTP**; click the plus (+) icon and select **HTTPS**.

g. From the **Action** drop-down list, select **Deny**.

h. Click **OK**.

**STEP 7—Set the secondary tunnel as the back-up to the primary.**

In the device CLI, enter the following command:

```
set monitor-phase1 phase1_name
```

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.
- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Juniper SSG20: Create a Site-to-Site VPN Connection

The most basic concept for this method is configure the router with a site-to-site VPN connection and configure the device policy rules to send web-based traffic to the Web Security Service and ignore everything else. Depending on your geographical location, you must create at least two VPN gateways. This procedure provides basic configuration steps. It is likely that you have an existing Juniper SRX device configured in your network; therefore, slight alterations to the existing deployment might be required.

Deployment Notes

- NAT-T cannot be enabled on the router/firewall device. The Web Security Service does not support that configuration at this time. The device must have an external routeable IP address.
- Do not send Auth Connector traffic to the Web Security Service.

**Note:** Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4) hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. *The screenshots in the following procedure might not reflect this advisory.*

Procedure

**Prerequisite A—Verify that the router is ready for configuration.**

a. Select Network > Interfaces > List.

b. Verify the list has as many interface pairs as required, plus the management interface.

**Prerequisite B—Verify that supported Phase 1 (encryption) and Phase 2 (authentication) Proposals exist.**


a. Select VPNs > AutoKey Advanced > P1 Proposal and check the list.

b. Select AutoKey Advanced > P2 Proposal and check the list.

**Step 1—Create the primary VPN Web Security Service gateway.**

1. Select VPNs > Autokey Advanced > Gateway.

2. Click New. The device displays the VPNs > Autokey Advanced > Gateway > Edit page.

3. Configure gateway settings.
a. **Name** the connection to the Web Security Service. For example, **ThreatPulseIP1**.

b. Select **IKEv1**.

c. Select **Static IP Address**.

d. Enter the primary Web Security Service **IP Address**. (refer to your planning sheet).

**TRANS-PROXY ALTERNATIVE:**

- For Trans-Proxy deployments, refer to "About Trans-Proxy (Explicit Proxy Over IPsec)" on page 20 for options; then proceed to sub-step 5.

e. Click **Advanced** to display more configuration options.

a. Enter the **Preshared Key**, which is the string that validates the encrypted tunnel between the router and the Web Security Service (refer to your planning sheet).

**Tip:** The PSK must be at least eight characters and **cannot** use special characters.

b. **Security Level** area:
   - Select the **Custom** option.
   - Select a supported **Phase 1 Proposal** encryption (see **Prerequisite** B above).

c. Verify that the **Enable NAT-Traversal** option is cleared.

d. Select **DPD** and set the **Interval** to any non-zero value. This is required for data center failover.

e. Click **Return** to go back to the **VPNs > Autokey Advanced > Gateway > Edit** page.

5. Click **OK**.
6. Repeat these Sub-steps 2-5 to create a VPN Gateway (example name: **ThreatPulseIP2**) for each additional Web Security Service IP Address.

**Step 2—Create a VPN group that will contain both gateways. This provides fail-over.**

1. Select **VPNs > Autokey Advanced > VPN Groups**.

   ![VPN Group ID Table]

   - **VPN Group ID**: 2
   - **Add** button
   - **ID** column
   - **Members** column
   - **Configure** column

2. Enter a new **VPN Group ID**.
3. Click **Add**.

**Step 3—Create a VPN tunnel.**

1. Select **VPNs > AutoKey IKE**.
2. Click **New**. The device displays the **VPNs > AutoKey IKE > Edit** page.
3. Assign the VPN to the gateway.

![VPN Tunnel Configuration]

- **VPN Name**: ThreatPulseVPN1
- **Remote Gateway**
- **Predefined**
- **Create a Simple Gateway**
- **Gateway Name**
- **Version Type**: IKEv1, IKEv2
- **Address/Hostname**
- **Peer ID**
- **User**: None
- **Group**: None
- **Local ID** (optional)
- **Preshared Key**
- **Security Level**: Standard, Compatible, Basic
- **Outgoing Interface**: ethernet0/1
- **ACVPN-Dynamic**
- **ACVPN-Profile**
- **Gateway**: None
- **Tunnel Towards Hub**: None
- **Binding to Tunnel**: None
- **Use As Seed**: checkbox
- **ACVPN-Profile**

Click **OK** or **Cancel**.
a. **Name** the VPN. For example: *ThreatPulseVPN1*.

b. **Remote Gateway** area—Select the **Predefined** option and from the drop-down list select the primary VPN gateway that you created in **Step 2**.

c. Select the **Outgoing Interface**, which is the untrusted interface (route to the Web Security Service).

d. Click **Advanced** to display more configuration options.

4. Configure the **User Defined** and **Replay Protection** options and assign to a **VPN Group**.

   ![VPN Configuration Screen]

   a. Select the **User Defined: Custom** option and select a supported **Phase 2 Proposal** authentication (see **Prerequisite B** above).

   b. Select **Replay Protection**.

   c. Select the **VPN Group** that you created in **Step 4**.

   d. Click **Return**.

**Step 4**—If your region requires more than one Web Security Service IP address,
repeat Step 3 to create another VPN tunnel with a Weight value of 2. For example, ThreatPulseVPN2.

If your planning form only lists one IP address for your region, skip to Step 5.

1. Assign it to the same **VPN Group** (this provides the failover capability).
2. Enter 2 for the **Weight** value (on the **Advanced** page, next to the **VPN Group** setting).

**Step 5—Verify VPN Group affiliation.**

1. Select **VPNs > Autokey Advanced > VPN Groups.**
2. Verify that the VPN group that you created contains the to VPN services.

<table>
<thead>
<tr>
<th>VPN Group ID</th>
<th>Members</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cloud1(weight:2), cloud2(weight:1)</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>ThreatPulseVPN1(weight:1), ThreatPulseVPN2(weight:2)</td>
<td>Remove</td>
</tr>
</tbody>
</table>

**Step 6—Define the Trust to Untrust policies for HTTP and HTTPS traffic.**

1. Select **Policy > Policies.**
2. The top of the page contains two drop-down lists: **From** and **To**.

   a. **From**—Select **Trust**.
   b. **To**—Select **Untrust**.
   c. Click **New**. The device displays the zone policy configuration screen.
3. Assign the internal subnet **HTTP** service to the **Tunnel VPN Group**.
Firewall/VPN Access Method Guide: Juniper SSG20: Create a Site-to-Site VPN Connection/Page 166

<table>
<thead>
<tr>
<th>Name (optional)</th>
<th>ThreatPulseHTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>![Image] Internal_subnet</td>
</tr>
<tr>
<td>Destination Address</td>
<td>![Image] Internal_subnet</td>
</tr>
<tr>
<td>Service</td>
<td>HTTP</td>
</tr>
<tr>
<td>Application</td>
<td>None</td>
</tr>
<tr>
<td>Action</td>
<td>Tunnel</td>
</tr>
<tr>
<td>Tunnel</td>
<td>![Image] VPN Group - 2</td>
</tr>
</tbody>
</table>

a. **Name** the policy. For example, **ThreatPulseHTTP**.

b. For the **Source Address**, select the **Internal_subnet** option from the **Address Book**.

c. The **Destination Address** setting depends on the Access Method:
   - For stand-alone IPsec deployments, select **any**.
   - For trans-proxy deployments, enter the Symantec Web Security Service explicit proxy IP address: **199.19.250.205**.

d. For the **Service** option, select **HTTP**.

e. For the **Action** option, select **Tunnel**.

f. Select the **VPN Group** that you created in **Step 2**.

g. Click **OK** to add the policy.

4. Repeat this step to create a **Trust** to **Untrust** policy for the **HTTPS** service.

**Step 7**—Create a **Trust** to **Untrust** rule that performs network address translation (NAT) on all other traffic.

Click **New**. The zone policy configuration screen displays.
a. **Name** the object.

b. For the **Source Address**, select the **Internal_subnet** option from the **Address Book**.

c. The default **Destination Address** is **Any**.

d. For the **Service** option, select **Any**.

e. For the **Action** option, select **Permit**.

f. For the **Tunnel: VPN** option, select **None**.

g. Click **OK**.

The SSG20 is now configured to route web traffic to the Web Security Service.

---

**Next Selection**

- Trans-Proxy deployment: Add the explicit proxy entry to PAC file. See "Add Explicit Proxy Entry to PAC File (Trans-Proxy)" on page 110.

- Stand-alone IPsec deployment: Proceed to "Add a Gateway Firewall/VPN Location" on page 169.
Perform an Admin Task

This section provides additional admin tasks.

- "Add a Gateway Firewall/VPN Location" on the next page
- "Verify Service Connectivity to Locations" on page 171
- "Forward Specific User and Group Names to the Service" on page 175
Add a Gateway Firewall/VPN Location

Each supported router/firewall device that is configured to send web traffic (VPN to VPN) to the Symantec Web Security Service requires an equivalent location configured in the service portal interface.

1. In Service Mode, select **Network > Locations**.
2. Click **Add Location**.
3. In the Add Location dialog, 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 of the router interface used to communicate to the Web.
   d. Enter the **Authentication Key** (pre-shared key) used to authenticate communication from the router.
4. Enter resource and location information.
a. Select the **Estimated User** range that will be sending web requests through this gateway interface. Symantec uses this information to ensure proper resources.

b. Select a **Country** and **Time Zone**.

c. Fill out location information and enter comments (optional).

5. Click **Save**.

- The Firewall/VPN Access Method supports Captive Portal.
  - See Set Auth Surrogate Types and Refresh.
Verify Service Connectivity to Locations

After configuring access to the SymantecWeb Security Service, verify that the service is receiving and processing content requests.

All Locations

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Connection Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>The Web Security Service recognizes the location and accepts web traffic.</td>
</tr>
<tr>
<td>🔄</td>
<td>A location has been configured, but the Web Security Service cannot connect. Verify that the web gateway device is properly configured to route traffic.</td>
</tr>
</tbody>
</table>
A previously successful web gateway to Web Security Service configuration is currently not connected.

- **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 Unified Agent—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 Unified Agent/Client Connector installation. See the section below for more information.

---

### Additional Step For Remote Users

To further verify that Unified Agent running on remote clients is communicating with the Web Security Service, click (or double-click) the application icon in the menu bar and click **Status**.

### Windows

![Blue Coat Unified Agent](image)
If the system detects a corporate network that provides web access and security, the Unified Agent enters into passive mode.

Mac

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

Next Steps

- Remote Users and Explicit Proxy Access Method—initial Configuration is complete.

Symantec also recommends adding private IP subnets to the IP bypass list to prevent internal traffic from routing to the Web Security Service service. For more information, see the How Do I? > Prevent IP/Subnet From Routing to the Service topic in Symantec Web Security Service WebGuide: Solutions
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 Symantec 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.

For large LDAP deployments, consider selecting which groups/users require Advanced Policy and forward only those names to the 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 Advanced 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 Web Security Service 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.

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:

   [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.
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 178
Troubleshoot IPsec/VPN/Firewall Connections

If you are having problems with IPsec/VPN/Firewall connections to the Symantec 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 Web Security Service IP address. "Plan the Device Configuration" on page 23

Verify that peer IP address is reachable from the router.

Can you ping the 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 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 Web Security Service supports only two types of Phase 2 proposals:

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

Access Method

Alter the access method (IPsec, Proxy Forwarding, Explicit Proxy) at the physical location.
Captive Portal Diagnostic Messages

When Captive Portal is enabled for remote clients on the Symantec Web Security Service, various messages are logged in association with user login activities and authentication. They display on the Service mode > Troubleshooting > Mobile Clients page.

<table>
<thead>
<tr>
<th>Log Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAResp&lt;0&gt; Captive Portal enabled: true</td>
<td>Indicates when Captive Portal was enabled (Service mode &gt; Network &gt; Mobility).</td>
</tr>
<tr>
<td>Captive portal authentication succeeded for username</td>
<td>Indicates when a user successfully logged in.</td>
</tr>
<tr>
<td>Authentication server error, connecting as unauthenticated user</td>
<td>If the Auth Connector becomes unavailable, the user receives the following error message: Authentication server error, connecting as unauthenticated user (also, Web Security Service adds the event to the diagnostic log). The behavior defaults to what happens when Captive Portal is not enabled. That is, the users' access credentials creates a tunnel. For diagnostic analysis, this Advanced dialog entry is unauthenticated (user_name).</td>
</tr>
<tr>
<td>Account restricted - CP auth failed for user: username</td>
<td>A user attempted to login in with incorrect credentials more times than the set limit in the Active Directory.</td>
</tr>
</tbody>
</table>