Configure Web Security

About the Web Security Module

The AnyConnect Web Security module is an endpoint component that routes HTTP traffic to a Cisco Cloud Web Security scanning proxy.

Cisco Cloud Web Security deconstructs the elements of a web page so that it can analyze each element simultaneously. For example, if a particular web page combined HTTP, Flash, and Java elements, separate "scanlets" analyze each of these elements in parallel. Cisco Cloud Web Security then allows benign or acceptable content and blocks malicious or unacceptable content based on a security policy defined in the Cisco ScanCenter management portal. This prevents "over blocking," where an entire web page is restricted because a minority of the content is unacceptable, or "under blocking," where an entire page is permitted while there is still some unacceptable or possibly harmful content that is being delivered with the page. Cisco Cloud Web Security protects users when they are on or off the corporate network.

With many Cisco Cloud Web Security scanning proxies around the world, users taking advantage of AnyConnect Web Security can route their traffic to the Cisco Cloud Web Security scanning proxy with the fastest response time to minimize latency.

You can configure the Secure Trusted Network Detection feature to identify endpoints that are on the corporate LAN. If this feature is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic is managed by other methods and devices on the corporate LAN rather than by Cisco Cloud Web Security.

AnyConnect Web Security features and functions are configured using the AnyConnect Web Security client profile, which you edit using the AnyConnect profile editor.

Cisco ScanCenter is the management portal for Cisco Cloud Web Security. Some of the components created or configured using Cisco ScanCenter are also incorporated in the AnyConnect Web Security client profile.

Note ISE servers must always be listed in the static exception list, which is configured on the Exceptions pane of the Web Security client profile.

Typical Web Security Configuration

Procedure

Step 1 Configure Cisco Cloud Web Security Scanning Proxies in the Client Profile.

Step 2 (Optional) Update the Scanning Proxy List if comparing the existing list of Cisco Cloud Web Security scanning proxies in the profile editor with those in the scanning proxylist downloaded from the http://www.scansafe.cisco.com/ website indicates a discrepancy.

Step 3 (Optional) Display or Hide Scanning Proxies from Users.

Step 4 Select a Default Scanning Proxy.

Step 5 (Optional) Specify an HTTP(S) Traffic Listening Port to filter HTTPS web traffic.

Step 6 Configure a host, proxy, or static exception to Excluding or Including Endpoint Traffic from Web Scanning Service. This configuration limits the evaluation of network traffic from the designated IP addresses.

Step 7 Configure User Controls and Calculate Fastest Scanning Proxy Response Time. This configuration chooses to which Cisco Cloud Web Security scanning proxy you want users to connect.

Step 8 If you want network traffic originating from the corporate LAN to bypass Cisco Cloud Web Security scanning proxies, Use Secure Trusted Network Detection.

Step 9 Configure Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy. This configuration authenticates users based on their enterprise domain or Cisco ScanCenter of Active Directory group.

Cisco Cloud Web Security Scanning Proxies in the Client Profile

Cisco Cloud Web Security analyzes web content, allowing delivery of benign content to your browser and blocking malicious content based on a security policy. A scanning proxy is a Cisco Cloud Web Security proxy server on which Cisco Cloud Web Security analyzes the web content. The Scanning Proxy panel in the AnyConnect Web Security profile editor defines to which Cisco Cloud Web Security scanning proxies the AnyConnect Web Security module sends web network traffic.

Guidelines for IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wildcard is specified, IPv6 web traffic is sent to the scanning proxy. The scanning proxy performs a DNS lookup to see if there is an IPv4 address for the URL that the user is trying to reach. If the scanning proxy finds an IPv4 address, it uses it for the connection. If no IPv4 address is found, the connection is dropped.

To enable all IPv6 traffic to bypass the scanning proxies, add ::/0 static exception for all IPv6 traffic. This exception makes all IPv6 traffic bypass all scanning proxies; therefore, IPv6 traffic is not protected by Web Security.

Note On devices that run Windows, if AnyConnect cannot determine the user ID, the internal IP address is used as the user ID. For example, if the enterprise_domains profile entry is not specified, use the internal IP address to generate reports in Cisco ScanCenter.

On devices that run macOS, the Web Security module can report the domain that device is logged in to, if it is bound to a domain. If it is not bound to a domain, the Web Security module can report the IP address of the device or the username that is currently logged in.

How Users Choose Scanning Proxies

Depending on how their profile is configured, users may choose a scanning proxy, or the AnyConnect Web Security module connects them to the scanning proxy with the fastest response time.

- If their client profile allows user control, users can select a scanning proxy from the Settings tab of the Cisco AnyConnect Secure Mobility Client Web Security tray.
- If their client profile has the Automatic Scanning Proxy Selection preference enabled, AnyConnect Web Security orders the scanning proxies from fastest to slowest and connects users to the scanning proxy with the fastest response time.
- If their client profile does not allow for user control but **Automatic Scanning Proxy Selection** is enabled, AnyConnect Web Security switches users from their default scanning proxy to the scanning proxy with the fastest response time, provided that the response time is significantly faster than the default scanning proxy to which they originally connected.
- If users start to roam away from their current scanning proxy and **Automatic Scanning Proxy Selection** is configured in their client profile, AnyConnect Web Security switches users to a new scanning proxy, provided that its response time is significantly faster than their current scanning proxy.

Users know the scanning proxy to which they are connected because AnyConnect Web Security displays the enabled scanning proxy name in the expanded AnyConnect tray icon on Windows, the Advanced Settings tab, and the Advanced Statistics tab of the AnyConnect GUI.

Update the Scanning Proxy List

The Scanning Proxy list in the Web Security profile editor is not editable. You cannot add or remove Cisco Cloud Web Security scanning proxies from the table in the Web Security profile editor.

After you start the Web Security profile editor, it updates the scanning proxy list automatically by contacting a Cisco Cloud Web Security website, which maintains the current list of scanning proxies.

When you add or edit an AnyConnect Web Security client profile, the profile editor compares the existing list of Cisco Cloud Web Security scanning proxies to those in the scanning proxy list that http://www.scansafe.cisco.com downloaded. If the list is out of date, a “Scanning Proxy list is out of date” message and command button labeled Update List appear. Click **Update List** to update the scanning proxy list with the most recent list of Cisco Cloud Web Security scanning proxies.

When you click Update List, the profile editor maintains as much of your existing configuration as possible. The profile editor preserves your default scanning proxy setting and the display/hide settings for the existing Cisco Cloud Web Security scanning proxies.

Display or Hide Scanning Proxies from Users

After users establish a VPN connection to the ASA, the ASA downloads a client profile to the endpoint. The AnyConnect Web Security client profile determines which Cisco Cloud Web Security scanning proxies are displayed to users.

For the maximum benefit to roaming users, we recommend that you display all Cisco Cloud Web Security scanning proxies to all users.

Users interact with the scanning proxies marked "Display" in the scanning proxy list of the AnyConnect Web Security client profile in these ways:

- The Cisco Cloud Web Security scanning proxies are displayed to users in the Advanced settings of the Web Security panel of their Cisco AnyConnect Secure Mobility Client interface.
- The AnyConnect Web Security module tests Cisco Cloud Web Security scanning proxies marked "Display" when ordering scanning proxies by response time.
- Users can choose which Cisco Cloud Web Security scanning proxy they connect to if their profile allows for user control.
- Cisco Cloud Web Security scanning proxies marked "Hide" in the scanning proxy table of the AnyConnect Web Security client profile are not displayed to users or evaluated when ordering scanning proxies by response time. Users cannot connect to the scanning proxies marked "Hide."

Before you begin

Create an AnyConnect Web Security client profile.

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile to edit.

Step 3 To hide or display Cisco Cloud Web Security scanning proxies:

- Choose the scanning proxy to hide and click Hide.
- Choose the name of the scanning proxy that you want to display and click Display. Displaying all Cisco Cloud Web Security scanning proxies is the recommended configuration.

Step 4 Save the AnyConnect Web Security client profile.

Select a Default Scanning Proxy

When users first connect to the network, they are routed to their default scanning proxy. By default, the profile that you create has the following Cisco Cloud Web Security scanning proxy attributes:

- The scanning proxy list is populated with all the Cisco Cloud Web Security scanning proxies that your users have access to, and they are all marked "Display."
- A default Cisco Cloud Web Security scanning proxy is pre-selected.
- The list of ports on which the AnyConnect Web Security module listens for HTTP traffic is provisioned with several ports.

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile to edit.

Step 3 Select a default scanning proxy from the **Default Scanning Proxy** field.

Step 4 Save the AnyConnect Web Security client profile.

Specify an HTTP(S) Traffic Listening Port

The Scan Safe web scanning service analyzes HTTP web traffic by default, and you can filter HTTPS web traffic through configuration. In the Web Security client profile, specify which ports you want Web Security to "listen" to for these types of network traffic.

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile to edit.

Step 3 In the **Traffic Listen Port** field, enter the logical port number that you want the Web Security module to "listen" to for HTTP traffic, HTTPS traffic, or both.

Step 4 Save the Web Security client profile.

Configuring Windows Internet Options to Configure Public Proxy

Public proxies are usually used to anonymize web traffic. Public proxy servers are referred to as authenticating proxy servers and may require a username and password. AnyConnect Web Security supports two types of authentication: basic and NTLM. When the proxy server is configured to require authentication, AnyConnect Web Security detects the proxy at run time and manages the authentication process. After successfully authenticating to the proxy server, the AnyConnect Web Security routes web traffic via public proxy to the Cisco Cloud Web Security scanning proxy. AnyConnect Web Security encrypts the proxy credentials, caches it securely in memory, and does not require credentials again, even if the user goes from proxy to non-proxy network and comes back to the same network. No service restart is required to work with public proxy. When a user moves to a non-proxy network, AnyConnect Web Security detects it automatically at runtime and starts sending web traffic directly to Cisco Cloud Web Security scanning proxy.

When Windows Internet options are configured to use a public proxy on a client, AnyConnect uses that connection.

Note Basic and NTLM public proxy are supported on Windows. Only Basic public proxy is supported on macOS.

1. Open Internet Options from Internet Explorer or the Control Panel.
2. Choose the Connections Tab and click **LAN settings**.
3. Configure the LAN to use a proxy server.
4. Enter the IP address or hostname of the proxy server. If separate proxies are configured for FTP/HTTP/HTTPS, only HTTPS proxy is considered.

Limitations

- IPv6 and TND behind public proxies are not supported.
- Proxy IP should not be in the AnyConnect Web Security exception list; otherwise, traffic will not be directed to the AnyConnect Web Security.
- If proxy port is different from the default web port, then the proxy port needs to be added in the kdf listening port list of the AnyConnect Web Security profile.

Excluding or Including Endpoint Traffic from Web Scanning Service

To exclude or include specific network traffic from Cisco Cloud Web Security scanning, use the Web Security profile editor to configure exceptions for that traffic. Several categories of exceptions can be configured:

- Host Exceptions or Host Inclusions—With Host Exceptions configured, the IP addresses (either public or private, host names, or subnets) that you enter are bypassed. With Host Inclusions configured, the IP addresses (either public or private, host names, or subnets) that you enter are forwarded to the Web Security proxy, while all remaining traffic is bypassed.

  Note AnyConnect can still intercept traffic that is listed in Host Exceptions.

- Proxy Exceptions—Internal proxy servers listed here are excluded from scanning.

- Static Exceptions—IP addresses listed here are excluded from scanning and AnyConnect.
-

ISE Server Requirements

ISE servers must always be listed in the static exception list, which is configured on the Exceptions pane of the Web Security client profile. In addition, the Web Sec module must bypass ISE Posture probes so the ISE Posture client to reach the ISE server. The ISE Posture profile sends network probes to find the ISE server in the following order:

1. Default gateway
2. Discovery host
3. enroll.cisco.com
4. Previously connected ISE server

Exclude or Include Host Exceptions

Before you begin

- Do not use wildcards on both sides of a top-level domain, for example *.cisco.*, because this could include phishing sites.
- Do not delete or change any of the default host exception entries.

You can choose to configure either Host Exceptions or Host Inclusions. If you choose Host Exceptions, the specified IP addresses are bypassed by the Cisco Cloud Web Security proxy. If you choose Host Inclusions, the specified IP addresses are forwarded to Cisco Cloud Web Security proxy while all other traffic is bypassed. Note that AnyConnect may still intercept internet traffic from an excluded host exception. To exclude traffic from both Web Security and AnyConnect, configure a Static Exception.

Procedure

Step 1 Choose Host Exceptions or Host Inclusions.

Step 2 Add the IP addresses (either public or private, host names, or subnets) that you want to bypass or forward, depending on your choice in Step 1.

Step 3 Enter subnets and IP addresses using the following syntax:

Syntax	Example
Individual IPv4 and IPv6 addresses	10.255.255.255 2001:0000:0234:C1AB:0000:00A0:AABC:003F
Classless Inter-Domain Routing (CIDR) notation	10.0.0.0/8 2001:DB8::/48

Fully qualified domain names	windowsupdate.microsoft.com ipv6.google.com **Note** Partial domains are not supported; for example, example.com is not supported.
Wildcards in fully qualified domain names or IP addresses	127.0.0.* *.cisco.com

Note When WebSecurity is configured to use domain names in the host exception list, a user may be able to spoof the host HTTP header entry in order to bypass the Web Security Proxies. This risk can be mitigated by using IP addresses instead of hostnames in the exception list.

Exclude Proxy Exceptions

In the Proxy Exceptions area, enter the IP addresses of authorized internal proxies (for example: `172.31.255.255)`.

You can specify IPv4 and IPv6 addresses in the field, but you cannot specify a port number with them. You cannot specify IP addresses using CIDR notation.

Specifying IP addresses prevents Cisco Cloud Web Security from intercepting web data bound for these servers and tunneling the data through them using SSL. Proxy servers can then operate without disruption. If you do not add your proxy servers here, you see Cisco Cloud Web Security traffic as SSL tunnels.

If you want to exempt any browser traffic via proxy server, you must list those hostnames in Host Exceptions, so that they are not forwarded. You cannot only configure static exceptions for traffic flowing through proxies not listed in the Proxy Exception list.

For proxies not on this list, Web Security attempts to tunnel through them using SSL. Therefore, if your users are at a different company site that requires a proxy to get out of the network for Internet access, Cisco Cloud Web Security provides the same level of support as if they were on an open Internet connection.

Exclude Static Exceptions

Determine which traffic should bypass Cisco Cloud Web Security and add a list of individual IP addresses or IP address ranges in Classless Inter-Domain Routing (CIDR) notation. In the list, include the ingress IP addresses of your VPN gateways.

If you have multiple hostnames with the same IP address but only one of the hostnames is configured in the Static Exceptions list, Web Security exempts the traffic.

Private IP addresses described in http://www.ietf.org/rfc/rfc1918.txt are included in the static exception list by default.

Note If you have a proxy server with an IP address in one of the ranges of the static exception list, move that exception to the host exception list. For example, 10.0.0.0/8 appears in the static exception list. If you have a proxy at 10.1.2.3, move 10.0.0.0/8 to the host exception list; otherwise, traffic sent to this proxy bypasses Cloud Web Security.

You can specify IPv4 and IPv6 addresses or ranges of addresses using CIDR notation. You cannot specify fully qualified domain names or use wildcards in IP addresses. Correct syntax examples are as follows:

```
10.10.10.5
192.0.2.0/24
```

Note Add the IP addresses of your SSL VPN concentrators to the static exclusion list.

Configure User Controls and Calculate Fastest Scanning Proxy Response Time

To allow users to choose which Cisco Cloud Web Security scanning proxy they connect to, perform the following:

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile to edit.

Step 3 Click **Preferences**.

Step 4 Select **User Controllable**. (This is the default setting.) User Controllable determines if the user can change the Automatic Tower Selection and Order Scanning Proxies by Response Time settings in the AnyConnect interface.

Step 5 For Web Security to automatically select a scanning proxy, choose **Automatic Scanning Proxy Selection**. If you do this, **Order Scanning Proxies by Response Time** is selected automatically.

- If you select **Automatic Scanning Proxy Selection**, Web Security determines which scanning proxy has the fastest response time and automatically connects the user to that scanning proxy.
- If you do not select **Automatic Scanning Proxy Selection**, and you still have **Order Scanning Proxies by Response Time** selected, users are presented with a list of scanning proxies to which they can connect, ordered from fastest to slowest response time.
- If you do not select **Automatic Scanning Proxy Selection**, users are still free to enable this feature from the AnyConnect user interface, but once enabled, they cannot switch it off again.

  Note When you enable Automatic Scanning Proxy Selection, transient communications interruptions and failures can cause the active scanning proxy selection to change automatically. Changing the scanning proxy can sometimes be undesirable, causing unexpected behavior such as returning search results from a scanning proxy in a different country using a different language.

Step 6 If you selected **Order Scanning Proxies by Response Time**, configure the following settings for calculating which scanning proxy has the fastest response time.

- **Enable Test Interval**: The time, in hours and minutes, between running each performance test (2 minutes by default). Switch off the test interval to prevent the test from running by clearing the Enable Test Interval check box.
- **Test Inactivity Timeout**: The time, in minutes, after which Web Security suspends the response time test because of user inactivity. Web Security resumes the testing as soon as scanning proxies encounter connection attempts. You should not change this setting unless instructed to do so by customer support.

Note The **Ordering Scanning Proxies by Response Time** test runs continuously, based on the Test Interval time, with the following exceptions:

- Secure Trusted Network Detection is enabled and has detected that the machine is on the corporate LAN.
- The Web Security license key is missing or invalid.
- The user is inactive for a configured amount of time, and as a result, the Test Inactivity Timeout threshold has been met.

Step 7 Click to enable Secure Trusted Network Detection, which detects whens an endpoint is on the corporate LAN, either physically or by means of a VPN connection. If enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies.

Step 8 In the https field, enter the URL of each trusted server, then click **Add**. The URL may include the port address. The profile editor attempts to connect to the trusted server. If this is not possible, but you know the SHA-256 hash of the server's certificate, enter it in the **Certificate hash** box and click **Set**.

Step 9 Save the Web Security client profile.

What to do next

See the *ScanCenter Administrator Guide, Release 5.2*, for more information.

Use Secure Trusted Network Detection

The Secure Trusted Network Detection feature detects when an endpoint is on the corporate LAN, either physically or by means of a VPN connection. If the Secure Trusted Network Detection feature is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than Cisco Cloud Web Security.

Secure Trusted Network Detection verifies the client is connected to the corporate network using the SHA-256 hash (thumbprint) of an SSLcertificate on a server at a known URL (address, IP, or FQDN). The encryption algorithm used by the certificate does not matter but only an SHA-256 hash can be used.

If you choose not to use Secure Trusted Network Detection and you have any proxies on your network, for example Cisco Cloud Web Security Connector, you must add each proxy to the list of proxy exceptions in the Exceptions panel in profile editor.

Multiple Servers: If you define more than one server, then if the client fails to connect to the first server after two consecutive attempts, it tries the second server. After trying all the servers in the list, the client waits five minutes, and tries to connect to the first server again.

Note When operating from outside your internal network, Secure Trusted Network Detection makes DNS requests and attempts to contact the HTTPS server that you provisioned. Cisco strongly recommends the use of aliasing to ensure that the name and internal structure of your organization are not revealed through these requests by a machine being used outside your internal network.

Before you begin

- Exclude Proxy Exceptions
- You must configure Secure Trusted Network Detection for some third-party solutions, such as data loss prevention (DLP) appliances, which require traffic that is unaffected by Web Security.
- Ensure you have a direct connection to the server where the SSL certificate is hosted when editing the profile.

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile that you wish to edit.

Step 3 Click **Preferences** in the Web Security tree pane.

Step 4 Select **Enable Trusted Network Detection**.

Step 5 In the **https** field, enter the URL of each trusted server, then click **Add**. The URL may include the port address. The profile editor attempts to connect to the trusted server. If this is not possible, but you know the SHA-256 hash of the server's certificate, enter it in the **Certificate hash** box and click **Set**.

Note Trusted servers behind proxies are not supported.

Step 6 Save the Web Security client profile.

Not Using Secure Trusted Network Detection

If you choose not to use Secure Trusted Network Detection and you have any proxies on your network (for example, Cisco Cloud Web Security Connector), you must add each proxy to the list of proxy exceptions in the Exceptions panel of the profile editor.

Configure Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy

Before you begin

Switch Off and Enable Filters Using Windows, on page 19

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile that you wish to edit.

Step 3 Click **Authentication**.

Step 4 In the **Proxy Authentication License Key** field, enter the license key that corresponds to the company key, group key, or user key that you created in Cisco ScanCenter. To authenticate users based on their Enterprise domain, enter the company key that you created. To authenticate users based on their Cisco ScanCenter or Active Directory group, enter the group key that you created. By default the tag is empty. If it is left empty, Web Security operates in pass-through mode.

Step 5 Enter a **Service Password**. The default password for Web Security is websecurity. Change this password when customizing the profile. The password must contain only alphanumeric characters (a-z, A-Z, 0-9) and the following special characters, as other characters may be mistaken for control characters by the Windows command shell or may have special meaning in XML.

```
~ @ # $ % * - _ + = { } [ ] : , . ? /
```

With this password, a user with administrator privileges can stop the Web Security service. Users with or without administrator privileges can start the Web Security service without this password.

Step 6 Send the scanning proxy server Enterprise Domain information and Cisco Cloud Web Security or Active Directory group information with every HTTP request. The scanning proxy applies traffic filtering rules based on what it knows of the user's domain and group membership.

Note To send a custom username and custom group information for a user to the scanning server proxy, skip this step and go to Step 7. Also skip to Setp 7 if your enterprise does not use Active Directory.

a) Click **Enable Enterprise Domains**. In the list, click **All Domains**. When the All Domains option is selected, and the machine is on a domain, the domain that the user belongs to is matched, and the username and group membership information is sent to the Cisco Cloud Web Security scanning proxy. This option is useful for companies with more than one domain present.

b) Alternatively, click **Specify Individual Domains**.

Enter each domain name in NetBIOS format and click Add. For example, the NetBIOS format of `example.cisco.com` is cisco. Do not enter domain names using the DNS format: abc.def.com.

If you specify a domain name in the Enterprise Domain name field, Cisco Cloud Web Security identifies the currently logged-in Active Directory user, enumerates that user's Active Directory groups, and sends that information to the scanning proxy with every request.

c) In the Use list, click **Group Include List** or **Group Exclude List** to either include or exclude group information in HTTP requests to the Cisco Cloud Web Security scanning proxy. Values can be any substring of the string to be matched.

Group Include List. After selecting **Group Include List**, add the Cisco Cloud Web Security or Active Directory group names to the Group Include list. These group names are sent to the Cisco Cloud Web Security scanning proxy server with HTTP requests. If a request comes from a user in the specified enterprise domain, the HTTP request is filtered in accordance with the user's group membership. If the user has no group membership, HTTP requests are filtered using a default set of filtering rules.

Group Exclude List. To the **Group Exclude List**, add the Cisco Cloud Web Security or Active Directory group names. These group names are not sent to the Cisco Cloud Web Security scanning proxy server with HTTP requests. If the user belongs to one of the groups in the Group Exclude List, that group name is not sent to the scanning proxy server, and the user's HTTP requests are filtered either by other group memberships or, at the minimum, by a default set of filtering rules defined for users with no Active Directory or Cisco Cloud Web Security group affiliation.

Step 7 Click **Custom matching and reporting for machines not joined to domains** to send the scanning proxy server custom name.

a) In the list, click **Computer Name** to use the name of the computer. Alternatively, click **Local User** to use the local username. Alternatively, click **Custom Name** and enter a custom username. It could be defined by any string. If you do not enter a string, the IP address of the computer is sent to the scanning proxy server instead. This username or IP address is used in any Cisco ScanCenter reports that identify HTTP traffic from the custom user.

b) In the **Authentication Group** field, enter a custom group name of up to 256 alphanumeric characters and click **Add**.

When HTTP requests are sent to the scanning proxy server, if a custom group name was sent, and there is a corresponding group name on the scanning proxy server, the HTTP traffic is filtered by the rules associated with the custom group name. If no corresponding custom group is defined on the scanning proxy server, HTTP requests are filtered by the default rules.

If you only configured a custom username and no custom group, HTTP requests are filtered by the scanning proxy server default rules.

Step 8 Save the Web Security client profile.

Advanced Web Security Settings

The Advanced panel of a Web Security client profile exposes several settings that may help Cisco customer support engineers troubleshoot problems. You should not change the settings on this panel unless you are instructed to do so by customer support.

From the Advanced panel in the profile editor, perform the following tasks:

- Configure the KDF Listening Port, on page 14
- Configure How the Port Listens for Incoming Connections, on page 14

Configure the KDF Listening Port

The Kernel Driver Framework (KDF) intercepts all connections that use one of the traffic listening ports as their destination port and forwards the traffic to the KDF listening port. The web scanning service analyzes all the traffic forwarded to the KDF listening port.

Before you begin

You should not change this setting unless instructed to do so by customer support.

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile that you wish to edit.

Step 3 Click **Advanced** in the Web Security tree pane.

Step 4 Specify the KDF listening port in the **KDF Listen Port** field.

Step 5 Save the Web Security client profile.

Configure How the Port Listens for Incoming Connections

The service communication port is the port on which the web scanning service listens for incoming connections from the AnyConnect GUI component, and some other utility components.

Before you begin

You should not change this setting unless instructed to do so by customer support.

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.

- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Select the Web Security client profile that you wish to edit and click **Edit**. Click **Advanced** in the **Web Security** tree pane.

Step 3 Edit the **Service Communication Port** field.

Step 4 Save the Web Security client profile.

Note If you change the port from the default value of 5300, you must restart the Web Security service and the AnyConnect GUI component.

Configure When Timeout/Retries Occur

The connection timeout setting enables you to set the timeout before Web Security tries to access the Internet without using the scanning proxies. If left blank, it uses the default value of 4 seconds. This setting allows users to get access to paid network services faster without waiting for the timeout to happen before retrying.

Procedure

Step 1 Start the Web Security profile editor using one of the following methods:

- Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.
- In Stand-alone mode on Windows, choose **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** > **Web Security Profile Editor**.

Step 2 Open the Web Security client profile that you wish to edit.

Step 3 Click **Advanced** in the Web Security tree pane.

Step 4 Change the **Connection Timeout** field.

Step 5 Save the Web Security client profile.

DNS Lookup

The Advanced panel of the profile editor contains several fields for managing Domain Name Server lookups. These settings have been configured with optimal values for DNS lookups.

Guidelines

You should not change this setting unless instructed to do so by customer support.

Debug Settings

The Debug Level is a configurable field.

Guidelines

You should not change this setting unless instructed to do so by customer support.

Block and Allow Traffic

In the Connection Failure Policy list, select **Fail Close** to block traffic if a connection to the Cisco Cloud Web Security proxy server cannot be established. Alternatively, select **Fail Open** to allow traffic.

In the **When a captive portal is detected** list, select **Fail Open** to allow traffic if a connection to the Cisco Cloud Web Security proxy server cannot be established but a captive portal, such as a Wi-Fi hot spot, is detected. Alternatively, select **Fail Close** to block traffic.

Note If host, proxy, or static exceptions are configured to include the captive portal address, then **Fail Close** will not block traffic.

Other Customizable Web Security Options

Export Options

Export the Plain Text Web Security Client Profile File

Export the obfuscated Web Security client profile from the ASA and distribute it to endpoint devices.

Procedure

Step 1 Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.

Step 2 Select the Web Security client profile that you wish to edit and click **Export**.

Step 3 Browse to a local folder to save the file. Editing the filename in the Local Path field saves the Web Security client profile with that new filename.

Step 4 Click **Export**.

ASDM exports the plain text `filename.wsp` version of the Web Security client profile.

Export the Plain Text Web Security Client Profile File for a DART Bundle

If you need to send a Diagnostic AnyConnect Reporting Tool (DART) bundle to Cisco customer service, send the plain text version of the Web Security client profile file (`filename.wsp` or `filename.xml`) along with the DART bundle. Cisco customer service cannot read the obfuscated version.

The stand-alone version of the profile editor creates two versions of the Web Security profile file: one file is obfuscated with the file name `filename.wso`, and the other is in plain text with the file name `filename.xml`.

Before sending the DART bundle to Cisco customer service, add the plain text version of your Web Security client profile to the DART bundle.

Edit and Import Plain Text Web Security Client Profile Files from ASDM

When you have exported the plain text Web Security client profile file, edit it on your local computer using any plain text or XML editor that allow edits not supported by the AnyConnect Web Security profile editor. You should not change the plain text version of the Web Security client profile unless instructed to do so by customer support. Use this procedure to import the editor.

Before you begin

Importing the file overwrites the contents of the Web Security client profile that you selected.

Procedure

Step 1 Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.

Step 2 Select the Web Security client profile that you wish to edit and click **Export**.

Step 3 After making the changes to `filename.wsp`, return to the AnyConnect Client Profile page and select the profile name of the file that you edited.

Step 4 Click **Import**.

Step 5 Browse to the edited version of the Web Security client profile and click **Import**.

Export the Obfuscated Web Security Client Profile File

Procedure

Step 1 Open ASDM and choose **Tools** > **File Management**.

Step 2 In the File Management screen choose **File Transfer** > **Between Local PC and Flash** and use the File Transfer dialog to transfer the obfuscated `filename.wso` client profile file to your local computer.

Configure Split Tunnel Exclusions for Web Security

When a user has established a VPN session, all network traffic is sent through the VPN tunnel. However, when AnyConnect users are using Web Security, the HTTP traffic originating at the endpoint needs to be excluded from the tunnel and sent directly to the Cloud Web Security scanning proxy.

To set up the split tunnel exclusions for traffic meant for the Cloud Web Security scanning proxy, use the **Set up split exclusion for Web Security** button in a group policy.

Before you begin

- Configure Web Security for use with the AnyConnect client.
- Create a group policy and assign it a connection profile for AnyConnect clients configured with Web Security.

If you use the Secure Trusted Network Detection feature and want to ensure that Web Security and VPN are active at the same time, configure your network so that the HTTPS server is not reachable over the VPN tunnel. In this way, the Web Security functionality goes into bypass mode, only when the user is on the corporate LAN.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2 Select a group policy and click **Edit** or **Add** a new group policy.

Step 3 Choose **Advanced** > **Split Tunneling.**

Step 4 Click **Set up split exclusion for Web Security.**

Step 5 Enter a new, or select an existing, access list used for Web Security split exclusion. ASDM sets up the access list for use in the network list.

Step 6 Click **Create Access List** for a new list or **Update Access List** for an existing list.

Step 7 Click **OK**.

What to do next

When additional scanning proxies are added, update the unified access list that you created in this procedure with new information.

Use Cisco Cloud Web Security Hosted Profiles

Starting in AnyConnect release 3.0.4, the Cisco ScanCenter Hosted Configuration for the Web Security Hosted Client Profile gives you the ability to provide new configurations to Web Security clients. Devices with Web Security can download a new Web Security Hosted Client Profile from the cloud (hosted configuration files reside on the Cisco ScanCenter server).

The AnyConnect client must also download its config files from the resource service through a hardcoded hostname in the AnyConnect binary. The request is made to **hostedconfig.scansafe.net/** (IP: 46.155.41.2). the exchange is encrypted over TCP port 443.

Hosted configuration allows access to the Ingress IP's of the CWS towers/proxies for AnyConnect Web Security via TCP port 443 (and also port 8080 in case of deploying in plain mode). The full list of towers/proxies for AnyConnect Web Security is available in the **Prepare** section of Cisco ScanCenter Administration Guide. The client must be able to access 80.254.145.118 on TCP port 80, where it fetches the list of proxy towers and keeps itself up to date. The Web Security module must be set to make connections to Verisign over TCP port 80. On this range, clients check the certificate of revocation at **TJ.symcb.com**, **T1.symcb.com**, and **T2.symcb.com** .

Use the Web Security profile editor to create the client profile files and then upload the clear text XML file to a Cisco ScanCenter server. This XML file must contain a valid license key, which has the same company, group, or user license key associated with the hosted configuration that was defined and hosted in Cisco Cloud Web Security. The client retrieves the new configuration file, at most, 8 hours after it is applied to the hosted configuration server.

The Hosted Configuration feature uses the license key when retrieving a new client profile file from the Hosted Configuration (Cisco ScanCenter) server. Once the new client profile file is on the server, devices with Web Security automatically poll the server and download the new client profile file, provided that the license in

the existing Web Security client profile is the same as a license associated with a client profile on the Hosted server. When a new client profile has been downloaded, Web Security will not download the same file again until you make a new client profile file available.

Refer to the *Cisco ScanCenter Administration Guide, Release 5.2*, for more information about license keys.

Before you begin

- Install the Web Security client device with a valid client profile that contains a Cisco Cloud Web Security license key.
- The restart Web Security agent service option is available only to users who have the necessary rights to restart the service.
- Client machines running the ACWS agent must have the Thawte Primary Root CA and Thawte SSL CA - G2 in the Trusted Root Certification Authority Store.

Procedure

Step 1 Using the Web Security profile editor, create a new client profile for the Web Security device. This client profile must contain the Cisco Cloud Web Security license key.

Step 2 Save the client profile file as a clear text XML file. Upload this file to the Cisco ScanCenter server. When the file is uploaded, make the new client profile available to Web Security clients.

Step 3 Upload the new client profile and apply it via the Cisco ScanCenter for the company, provided that the Hosted Configuration feature was enabled for the company. A hosted client profile is associated with a license. If different licenses are in use (for example, different group license keys), each license can have its own client profile associated with it. You can then push down a different client profile to different users, depending on which licenses they are configured for. You store various configurations per license and set a default client profile for clients to download. They can then switch to one of the other revisions of configurations stored in the Hosted Configuration area of Cisco ScanCenter by selecting that client profile as the default. A license is associated with only one client profile; therefore, you can have only one default when more than one revision is associated with the license.

Switch Off and Enable the Cisco AnyConnect Web Security Agent

You can switch off and enable the Cisco AnyConnect Web Security Agent's ability to intercept web traffic by executing the following steps.

Switch Off and Enable Filters Using Windows

Procedure

Step 1 Open a command prompt window.

Step 2 Go to the **%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** folder.

Step 3 Switch filtering on or off:

- To enable filtering, enter **`acwebsecagent.exe -enablesvc`**

- To disable filtering, enter **acwebsecagent.exe -disablesvc -servicepassword**

Switch Off and Enable Filters Using macOS

The service password is configured in the Authentication panel of the Web Security profile editor.

Procedure

Step 1 Launch the Terminal application.

Step 2 Go to the `/opt/cisco/anyconnect/bin` folder.

Step 3 Enable or switch off filtering:

- To enable filtering, enter **./acwebsecagent -enablesvc**.
- To disable filtering, enter **./acwebsecagent -disablesvc -servicepassword**.

Web Security Logging

Windows

All Web Security messages are recorded in the Windows Event Viewer in the `Event Viewer (Local)\Cisco AnyConect Web Security Module` folder. The events Web Security records in the event viewer are analyzed by Cisco Technical Assistance Center engineers.

macOS

View Web Security messages from the syslog or console.