

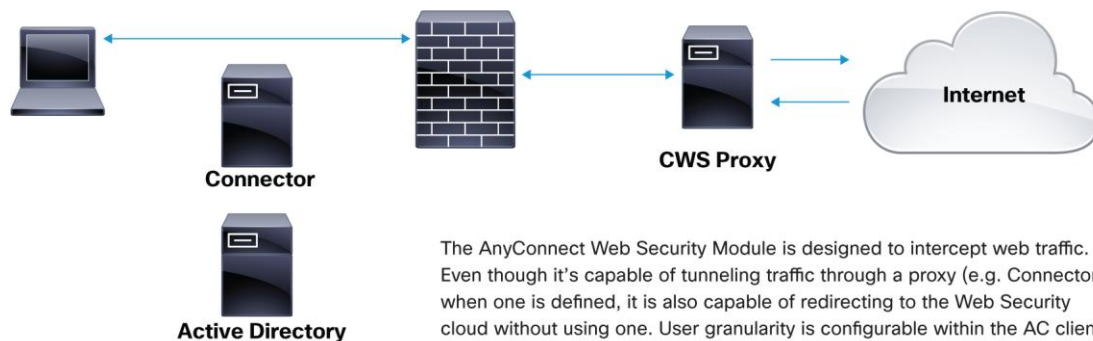
Cisco Cloud Web Security: AnyConnect for ASA Activation Guide



This document outlines the deployment of the Cisco Cloud Web Security (CCWS) service. Included are the deployment description, configuration checklist, and step-by-step video tutorials that detail all the steps necessary to successfully activate the Filtering and Scanning of Web traffic.

The Cisco AnyConnect Secure Mobility client can be deployed to remote users from the ASA. When using this method, remote users make an initial SSL connection to the ASA to obtain the client and/or any other needed modules (i.e. Web Security). In their browser, they enter the IP address or DNS name of an ASA configured to accept clientless SSL VPN connections. The ASA presents a login screen in the browser window and, if the user satisfies the login and authentication, downloads the client. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

Figure 1. AnyConnect Traffic Flow Interception



The AnyConnect Web Security Module is designed to intercept web traffic. Even though it's capable of tunneling traffic through a proxy (e.g. Connector) when one is defined, it is also capable of redirecting to the Web Security cloud without using one. User granularity is configurable within the AC client.

AnyConnect Web Security Module supports the following operating systems

- Windows XP SP3 x86 (32-bit)
- Windows Vista x86 (32-bit) or x64 (64-bit)
- Windows 7 x86 (32-bit) or x64 (64-bit)
- Mac OS X v10.5 x86 (32-bit)
- Mac OS X v10.6 x86 (32-bit) or x64 (64-bit)
- Mac OS X v10.7 x86 (32-bit) or x64 (64-bit)

AnyConnect Secure Mobility Client with the Web security module requires these minimum ASA components

- ASA 8.4(1)
- ASDM 6.4(0)104

AnyConnect Package to be hosted from the ASA

- Windows anyconnect-win-(ver)-k9.pkg
- Mac anyconnect-macosx-i386-(ver)-k9.pkg

Client Checklist

- Configure the firewall to allow port 443 outbound to the relevant Secure Mobility towers.
- Configure the firewall to allow port 80 outbound access to 80.254.145.118.
- ASA must be configured to accept AnyConnect VPN clients.
- Ensure that there is no rate limiting on the firewall that will prevent or hinder connections to the cloud proxy. This may be rate limiting or DoS Protection.
- Gather any supplier sites that are TCP wrapped, or rely on traffic originating from a static source IP and will not accept connections via the cloud proxies. These need to be noted for exception.
- Gather any internal or external domains or URLs that need exception.

Video Tutorials

Cisco Cloud Web Security Preparation

These videos are a good reference for gathering the needed items for the configuration.

1. [Authentication License Key Creation and Management](#)

Note: Prerequisite if Group Keys will be used – [How to Create and Manage Groups in the CCWS Portal](#)

Configuring the Secure Mobility Client

This video details the basic configuration of the Secure Mobility Client. The client will redirect traffic to the Cisco Cloud and can also be configured to obtain user information.

2. [Creating an AnyConnect Service Profile Using the Stand-alone Profile Editor](#)
3. [How to Install AnyConnect Web Security Using the Web-deploy Method](#)

ScanCenter Configuration

After traffic is successfully redirected and user credentials are being passed to the Cloud, it's time to configure the Web Filtering policy.

4. [How to Create and Manage Groups in the CCWS Portal](#)
5. [How to Manage and Configure Web Filtering Policy](#)
6. [Cisco Cloud Web Security Portal Overview](#)



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)