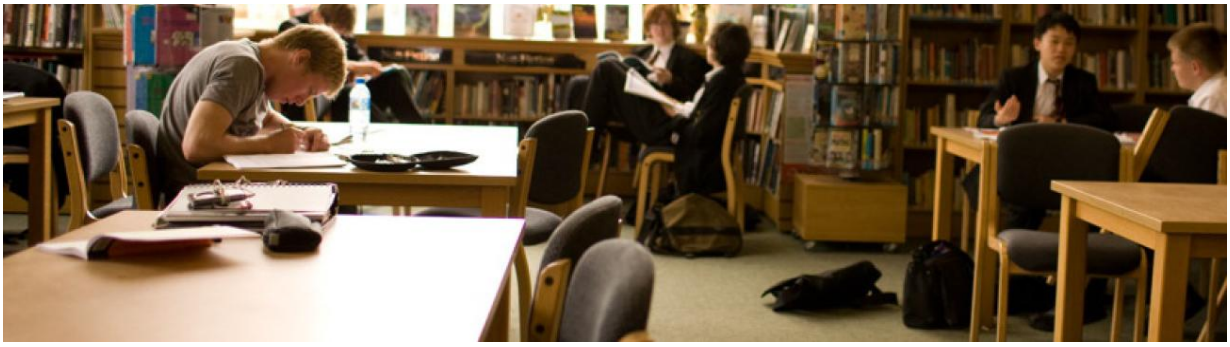
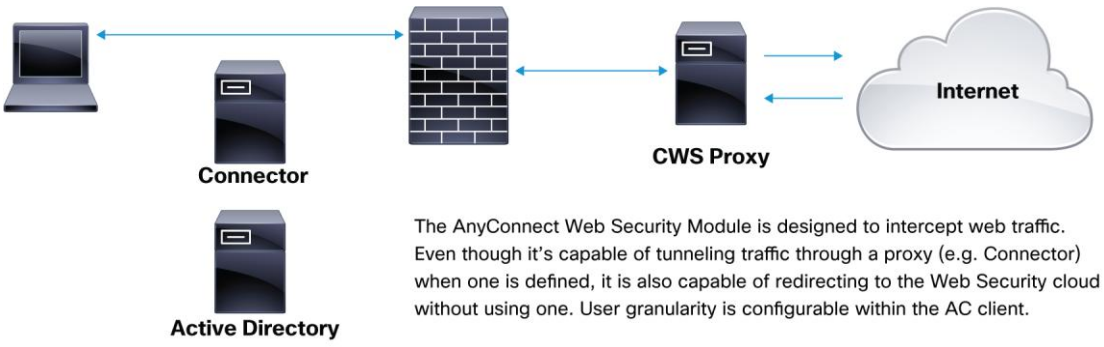
Cisco Cloud Web Security: AnyConnect Activation Guide



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.

This deployment method provides a roaming user the same protection and web policy outside of the office as when they are within the LAN being filtered and scanned. The Cisco AnyConnect Secure Mobility Client tunnels the traffic directly to the Cisco Cloud. End user granularity is configurable within the client itself. Since all web traffic is intercepted, you do not need to define proxy settings to redirect traffic to the Cisco Cloud.

Figure 1. AnyConnect Traffic Flow Interception



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)

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.
- Ensure that there is no rate limiting on the firewall that will prevent or hinder connections to our tower. 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 our towers. 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. It also reviews how to test basic connectivity.

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 Pre-deploy Method

Portal 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.**

Printed in USA C07-726149-00 01/13