



Combating Web-Based Threats Using Cisco WSA and CWS



Copyright © www.ine.com

Topic Overview

- ▶ Introduction To Web-Based Threats
- ▶ Contrasting Cloud-Based & Local Web Proxies
- ▶ Introducing The Cisco WSA & CWS
- ▶ WSA & CWS Traffic Flow

Web-Based Threats

▷ Some examples of web-based threats include;

- ▶ Requests for websites that break a stated Acceptable Use Policy (AUP)
- ▶ Known, malicious websites that install malware, spyware or viruses.
- ▶ Legitimate websites that have been compromised and download malware.
- ▶ Employees contributing to corporate Data Loss through unauthorized/unmonitored data uploads.



▷ Cisco's solutions for mitigating web-based threats;

- ▶ Cisco Cloud Web Security
- ▶ Cisco Web Security Appliance with integrated AMP technology

Cloud Or Local Web Proxies

- ▶ **Cloud-based solutions are considered SaaS solutions (Security as a Service).**
 - ▶ Negates the need for hardware maintenance or software upgrades
 - ▶ Can be accessed from corporate users, mobile users, and home teleworkers using a variety of software “connectors”.
 - ▶ Cisco solution: [Cisco Cloud Web Security](#)
- ▶ **On-premises solutions using hardware (or virtual) Appliances provide alternative benefits;**
 - ▶ Anonymity is preserved.
 - ▶ Complete control over your solution
 - ▶ Finer granularity over reporting and statistics
 - ▶ Cisco solution: [Cisco Web Security Appliance](#)

Copyright © www.ine.com



A web proxy is a device that intentionally intercepts web requests from clients, scans them for safety and corporate compliance, and then either forwards the requests to the destination server, or initiates requests to the server on behalf of the clients.

-
There are some downsides to cloud-based web-security solutions; All of your webtraffic must be sent to resources that are not in your direct control. This could break federal compliance restrictions or simply be a concern that you've lost a degree of anonymity. Also, if your network access to the cloud solution is temporarily unavailable, that could be a concern.

Introducing The Cisco WSA

▷ WSA = Web Security Appliance

- ▶ Web proxy device
- ▶ Monitors and controls outbound web requests for web content
- ▶ Scrubs return traffic for unwanted or malicious content

▷ Web traffic from clients, and responses from websites must be directed to the WSA;

- ▶ Explicit proxy configuration on clients
- ▶ WCCP to redirect traffic from network devices (Firewalls, Routers, etc)
- ▶ PBR or other methods



Copyright © www.ine.com

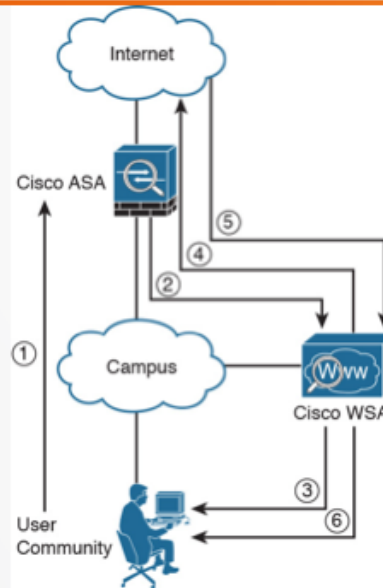


For outbound web requests, the WSA will intercept them and confirm that the request doesn't violate any corporate policy or is going to any known, malicious website.

-

Similar to the Cisco ESA, this appliance uses the Anysync OS (remember that both the ESA and WSA came to Cisco as a result of the IronPort acquisition).

WSA Traffic Flow



Copyright © www.ine.com



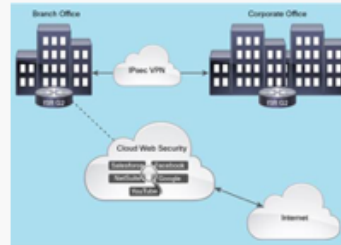
In this example, WCCP is being used between the Firewall and the WSA so that when the Firewall receives the user's web request, it is redirected to the WSA for inspection. At this point, the WSA initiates a connection to the website on behalf of the user and inspects all the content that is returned.

Step-3 of this graphic is illustrating how the WSA would respond with a denial message back to the user, if the user were trying to break corporate policy by attempting to access an unauthorized website. More details of this to follow.

Introducing Cisco CWS

▶ CWS = Cloud Web Security

- ▶ Cloud-based web proxy device
- ▶ Similar in functionality to Cisco WSA
- ▶ Web usage controls with category and reputation-based control, malware filtering, and data protection.



▶ Cisco CWS Datacenters;

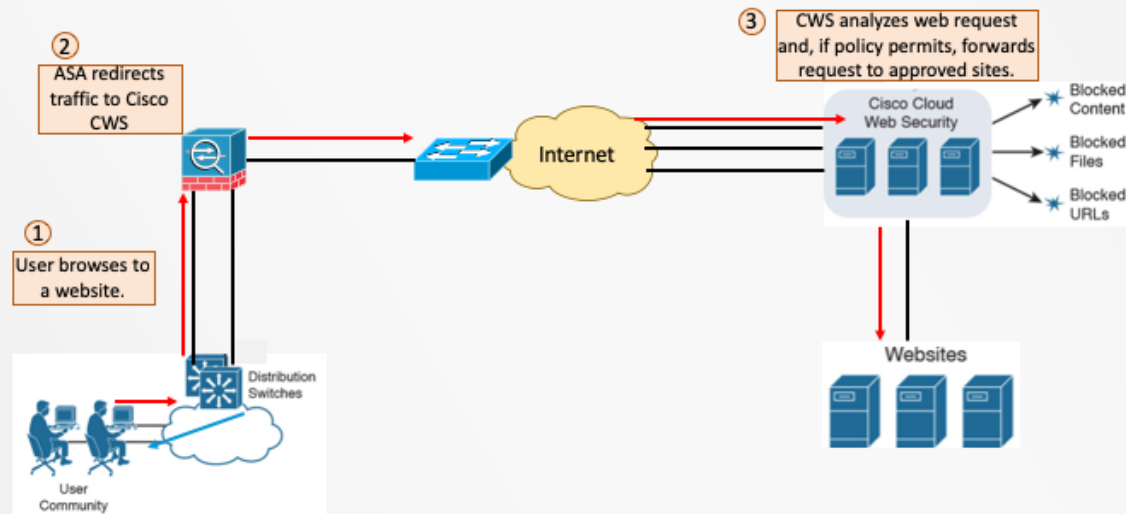
- ▶ Spread geographically all over the world
- ▶ Interconnected and redundant
- ▶ Can be used with Cisco AnyConnect Secure Mobility Client to provide web security for mobile and remote users.

Copyright © www.ine.com



Cisco CWS was formerly called ScanSafe.

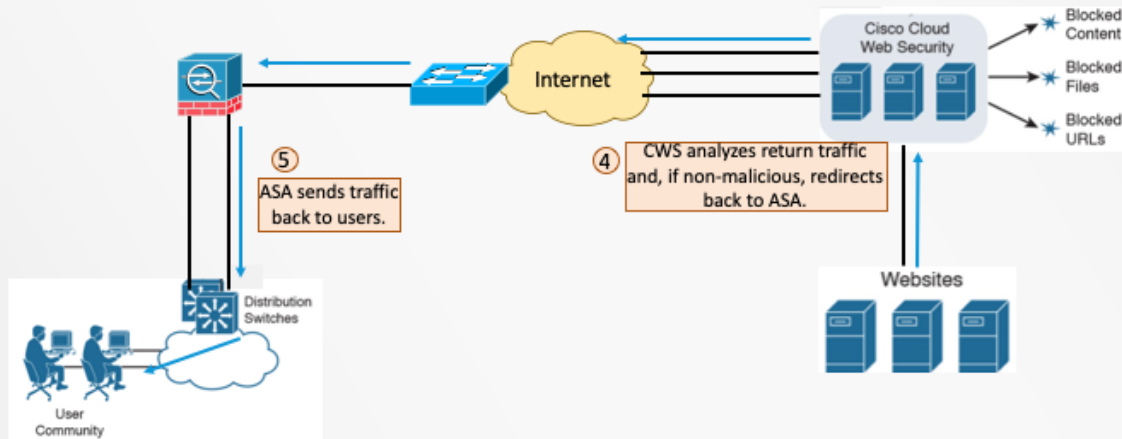
Cisco CWS Traffic Flow



Copyright © www.ine.com



Cisco CWS Traffic Flow





Introduction To WSA Features



Copyright © www.ine.com

Topic Overview

- ▶ URL Filtering, Blacklisting & Categorization
- ▶ Content Filtering & AMP
- ▶ L4TM & HTTPS Decryption
- ▶ DLP Features With The WSA
- ▶ WSA Configurable Actions For Web Requests

Copyright © www.ine.com



L4TM means Layer-4 Traffic Monitoring

URL Filters & Categorization

▶ URL Filtering & Blacklisting

- ▶ Category filtering with 79-predefined URL categories
- ▶ Custom URLs
- ▶ Dynamic content analysis and/or filtering of URL strings

▶ Some examples of commonly filtered pre-defined URL categories include:

Category	Abbreviation	Code	Description	Example URLs
Adult	adlt	1006	Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers); general information about sex, nonpornographic in nature; genital piercing; adult products or greeting cards; information about sex not in the context of health or disease.	http://www.adultentertainmentexpo.com http://www.adultnetline.com
Dating	date	1055	Dating, online personals, matrimonial agencies.	http://www.eharmony.com http://www.match.com
Hacking	hack	1050	Discussing ways to bypass the security of websites, software, and computers.	http://www.hackthissite.org http://www.gohacking.com
Hate speech	hate	1016	Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity; sites promoting racism; sexism; racist theology; hate music; neo-Nazi organizations; supremacism; Holocaust denial.	http://www.kkk.com http://www.nazi.org

Copyright © www.ine.com



URL filtering is based on an active database comprising the analysis of sites in 190 countries in over 50 languages.

-

A complete list of pre-defined categories can be found at

https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/datasheet_C78-718442.html

-

Blacklisting involves configuring the WSA with pre-defined URLs that you don't want your users to access.

Content Filtering & AMP

▶ Web Content Filtering

- ▶ Customized filters to control downloaded file-types.

▶ Anti Malware Content Filtering

- ▶ Leverages Cisco's Advanced Malware Protection (AMP) solution
- ▶ Requires additional add-on license to the WSA
- ▶ Reputation database maintained by Cisco Talos
- ▶ Updated every 5-minutes

What is the difference between URL filtering and Content filtering? URL filtering is done upstream (filtering out unacceptable URLs before sending the request to the web server). Content filtering is done downstream, by scanning files for certain filetypes that you have configured as unacceptable (like PDF files or .zip files).

Content Analysis & AUP Enforcement

▶ Dynamic Content Analysis

- ▶ Used to help determine category of newer websites that have not yet been categorized into Cisco's URL Categorization Database.
- ▶ Determines nature of content in real time using Cisco's DCA (Dynamic Content Analysis) Engine.
- ▶ Findings sent back to SenderBase repository if customer elects to do so

▶ Acceptable Use Policy (AUP) enforcement

Copyright © www.ine.com



How does the appliance validate the security of unknown/unrated sites? After checking the domain owner, the server where the site is hosted, the time the site was created, and the type of site, the site is assigned a reputation score. Based on that reputation score and selected security policies, the site is blocked, allowed, or delivered with a warning. Cisco Talos updates Web reputation filtering intelligence every 3 to 5 minutes.

-

Dynamic Content Analysis also applies to well-known websites that might host multiple types of content (like Pinterest) and don't easily fall into a single URL category. Sites like these can occasionally host malware or other unacceptable content (that comes and goes as postings occur or are taken down). Dynamic content analysis relies on people reporting this content into Cisco's SenderBase so that your WSA can be updated on a frequent basis of websites that might have been safe minutes ago...but are no longer reliable.

-

From Cisco documentation – "Cisco IronPort SenderBase collects data on more than 30 percent of the world's email and web traffic. A highly-diverse group of more than 120,000 organizations, including the largest networks in the world, contributes information to Cisco IronPort SenderBase on a remarkable 5 billion messages per day."

L4TM & HTTPS Decryption

▶ Layer 4 Traffic Monitor (L4TM)

- ▶ Utilized to prevent malware, that has already infected internal clients, from bypassing HTTP Port-80 and “phoning-home”.
- ▶ Maintains its own internal database

▶ Intelligent HTTPS decryption

- ▶ Must enable the “HTTPS Proxy” service on the WSA
- ▶ WSA creates the HTTPS session to the webserver and creates a new HTTPS session to the user.
- ▶ The responses from the webserver are checked and scanned and delivered over the new HTTPS session to the user.

Copyright © www.ine.com



L4TM: This is on by default. Utilizes a database (frequently updated and downloaded from Cisco) of known IP address, DNS names, and other information that malware utilizes when sending packets from infected Clients to the outside world. By default this feature only creates reports so you have visibility into what is going on in your network. Alternatively you could allow your WSA to block/stop traffic that L4TM flags as suspicious by sending TCP Reset messages or (for UDP traffic) ICMP Unreachable messages.

-

You might wonder, “how does the WSA decrypt HTTPS traffic”? Remember that the WSA initiates connections to HTTPS websites on your behalf. So the actual SSL/TLS exchange is happening between the WSA and the webserver.

-

There is one major drawback with enabling HTTP decryption: the WSA shows the user a SSL certificate of the WSA appliance itself (instead of the Cert of the website which the user’s browser is expecting to see). In almost all circumstances this certificate wouldn’t match all requirements, so the users receive SSL certificate errors. Make sure your users are familiar with your HTTPS inspection and some tweaking of their browser’s behavior will be necessary!

WSA DLP Features

- ▶ Data Loss Prevention by monitoring what is posted via HTTP, HTTPS or FTP
- ▶ Requires that the WSA work in partnership with another appliance, the Digital Guardian DLP Appliance.
- ▶ When uploading content to a website (Dropbox, Google Drive, FTP, etc) DLP policies can also be configured to allow or block content to a site.

Copyright © www.ine.com



Digital Guardian, a Cisco partner, offers a complete data loss prevention (DLP) solution. It uses content and context awareness to support complex use cases that involve intellectual property, trade secrets, customer lists, customer credit card information, and other data.

-

DLP by the WSA examples include preventing engineers from sending design files by webmail, blocking uploads by finance staff of Excel spreadsheets over 100 KB, or preventing posts of content to blogs or social networking sites.

DLP Protection

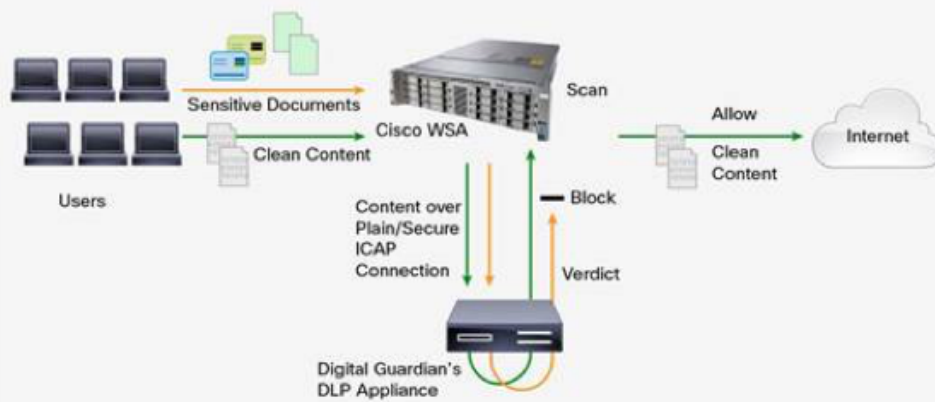


Image courtesy of: <https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-738537.html>

Copyright © www.ine.com



WSA Configurable Actions

- ▶ After scanning requests for outbound websites, or inbound web content, the Cisco WSA can take one of the following actions:
 - ▶ **Allow** the web content
 - ▶ **Warn** the user about a potentially malicious site or one that breaks the AUP
 - ▶ Entirely **block** all web content from a site

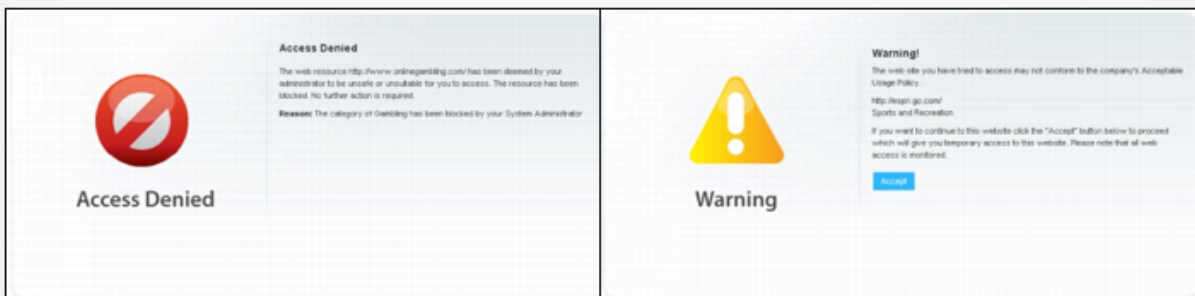
Copyright © www.ine.com



Remember that there is also a “partial block” option available for enforcing Data Loss Prevention (see previous slide).

WSA End-User Experience

- ▶ When the WSA is configured to block specific sites or content...or warn users that they may be about to break an AUP (Acceptable Use Policy) users will see one of the following:





WSA Deployment Options

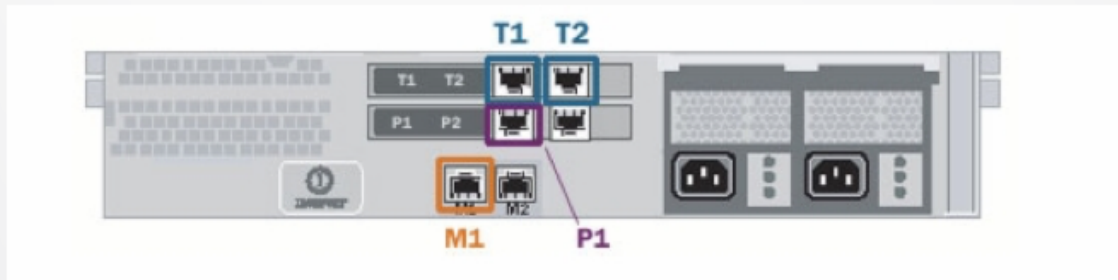


Copyright © www.ine.com

Topic Overview

- ▶ Methods Of Implementing Transparent Proxy
- ▶ Explicit Forward Proxy
- ▶ L4 Traffic Monitor

WSA Interfaces



The M1 port is used for managing the WSA. That can also be used as an additional data port.

-

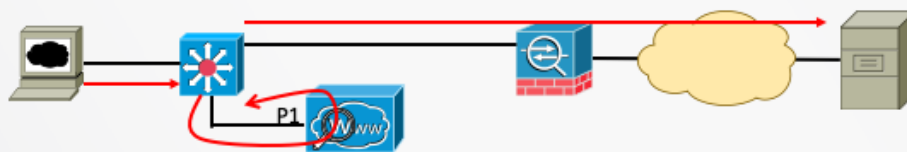
The P1 and P2 ports are used for sending/receiving redirected Web Traffic. Inspection and enforcement of web policies happen on these ports.

-

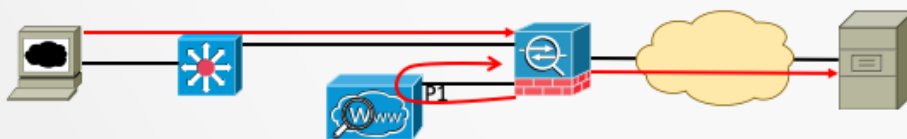
The T1 and T2 ports are used if you plan on (optionally) also implementing the Layer-4 Traffic Monitoring feature of the WSA.

WSA Deployment Options

▶ Transparent Proxy with L4 Switch



▶ Transparent Proxy with WCCP Router or Firewall



Copyright © www.ine.com



There are four deployment options for the WSA.

-

In both of these first two contexts, the words “transparent” means that end users have no idea the WSA exists and no special configuration must occur on the laptops or PCs.

-

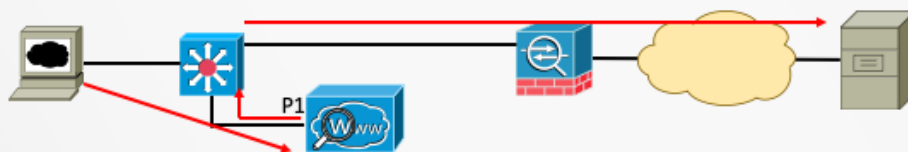
When using a Layer-4 switch to provide redirection, you would most likely implement Policy-Based Routing to match on ingress HTTP and HTTPS traffic and redirect that traffic to the WSA for inspection.

-

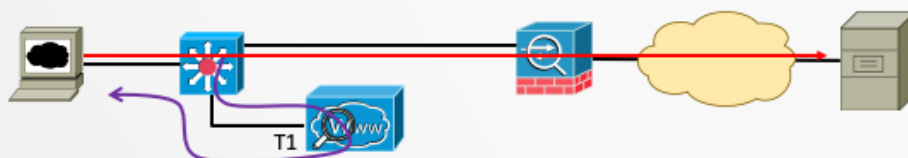
WCCP (the Web Cache Control Protocol) is a Cisco-proprietary protocol.

WSA Deployment Options

► Explicit Forward Proxy



► L4 Traffic Monitor



Copyright © www.ine.com



Note that using the WSA as a L4 Traffic Monitor is not an “or” solution but an “and” solution. You can use it as BOTH a L4 Traffic Monitor as well as normal WSA features. Keep in mind that the L4TM engine is a separate engine from all the other stuff that the WSA does. It doesn't have visibility to any data entering the WSA on the P1 and/or P2 ports. This is why data traffic from the web-clients (web lookups and website responses) must be directed to the P1 port(s) on the WSA...but that same traffic must be spanned/copied by the Switch and sent to the WSAs T1/T2 ports.

As an L4 Traffic Monitor the WSA would be connected to a SPAN port on the switch. So if it isn't operating in-line with the traffic but only receiving copied traffic...how does it block undesirable traffic? By sending either TCP reset messages back the to client, or ICMP Host Unreachable messages (in the case of UDP traffic). And these messages are transmitted out of the P1 port.

<https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117985-qanda-wsa-00.html>



Introduction To WCCP



Copyright © www.ine.com

Topic Overview

- ▶ What Is WCCP?
- ▶ WCCP With A Cisco WSA
- ▶ WCCP Server Basic Configuration
- ▶ WCCP Client Configuration (Cisco WSA)

Web Cache Communications Protocol

- ▶ Utilized to redirect Web request to another device (such as a Cisco Content Engine or WSA).
- ▶ Redirected packets encapsulated within GRE headers to prevent packet modification.
- ▶ Originally designed to localize traffic patterns in the network, enabling content requests to be fulfilled locally
- ▶ Cisco-proprietary protocol
- ▶ Two versions of WCCP exist (v1 and v2)
 - ▶ WCCPv2 supports protocols other than HTTP, multiple routers, MD5 security, and load distribution
 - ▶ WCCPv2 supports IPv6

Copyright © www.ine.com



When WCCP forwards traffic via GRE, the redirected packets are encapsulated within a GRE header. The packets also have a WCCP redirect header.

-

WCCP can also be configured to simply rewrite the L2 header if the WCCP Client-and-Server are on the same subnet.

WCCP With The WSA

- ▷ Cisco WSA is considered a WCCP Client
- ▷ Router (or Firewall) is the WCCP Server.
 - ▶ WCCP Registration Announcements sent from Client to Server every 10-seconds
 - ▶ WCCP Holdtime is 30-seconds on the WCCP Server



Image courtesy of, "CCNA Security 210-260 Official Certification Guide" by Cisco Press

Copyright © www.ine.com



WSA = Web Security Appliance

-

The WCCP Registration messages occur on UDP port 2048.

-

By default the WCCP Server (Router/Firewall) will only redirect HTTP (TCP Port 80) messages to the WSA. If using WCCP version 2 and you wish to redirect other protocols, configuration must be done on the WSA...which will inform the WCCP Server (Router/Firewall) which protocols it wishes to receive.

-

The nature of the selected traffic for redirection is defined by service groups specified on content engines/Web Security Appliances and communicated to routers by using WCCP.

WCCP Server Configuration

```
Router(config)# ip wccp version 2
Router(config)# ip wccp web-cache password mypassword
Router(config)# interface Fa0/0
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ^Z
```

```
Router# show ip wccp web-cache

Global WCCP Information:
Service Name: web-cache:
Number of Cache Engines:      1
Number of Routers:           1
Total Packets Redirected:     213
Redirect access-list: no_linux
Total Packets Denied Redirect: 88
Total Packets Unassigned:     -none-
Group access-list:            0
Total Messages Denied to Group: 0
Total Authentication failures: 0
```

Copyright © www.ine.com



As previously mentioned, WCCP “Service Groups” define what types of traffic will be redirected by a WCCP Server to a Client. The default Service Group is named “web-cache” and matches on all received HTTP traffic.

-

Notice that on the WCCP server there is no mention of the IP address of the WCCP Client. This will be learned dynamically by the WCCP Server upon receiving frequent-and-periodic WCCP Registration messages (also used as Hellos) sent from the WCCP Clients.

-

In the output of “show ip wccp web-cache” we see that one cache engine (which is just a generic term for a WCCP Client and could also be a Cisco WSA) has registered with this Router.

WCCP Client (WSA) Configuration

The screenshot shows the Cisco S100V Web Security Virtual Appliance configuration wizard. The title bar reads "Cisco S100V Web Security Virtual Appliance". Below the title bar is a progress bar with four steps: 1. Start, 2. Network (selected), 3. Security, and 4. Review. The main content area is titled "Transparent Connection Settings" and contains the following text: "For the Cisco Web Security Appliance to accept transparent connections, it must be connected via a Layer 4 switch or WCCP router." Below this text is a section for "Transparent Redirection Device:" with two radio button options: "Layer 4 Switch or No Device" (selected) and "WCCP v2 Router". Under the "Layer 4 Switch or No Device" option, there is a checkbox for "Enable standard service ID: 0 web_cache (port 80)". Under the "WCCP v2 Router" option, there is a text field for "Router Addresses:" with a note "Separate multiple addresses with commas or whitespace." Below this is a checkbox for "Enable router security for this service". Under this checkbox, there are two text fields: "Password:" and "Confirm Password:", with a note "Must be 7 or less characters." At the bottom of the form, there is a note: "Additional WCCP services and advanced options can be configured after completing the System Setup Wizard." At the bottom left of the form are buttons for "< Prev" and "Cancel". At the bottom right is a button for "Next >".

Copyright © www.ine.com



In this screen we see part of the setup wizard one initially goes through when configuring the WSA. On the "Network" tab you are given basic options to enable WCCP.

WCCP Client (WSA) Configuration

Add WCCP v2 Service

Error — Errors have occurred. Please see below for details.

WCCP v2 Service

Service Profile Name:

Service:

- ☐ Standard service ID: 0 web-cache (destination port 80)
- ☒ Dynamic service ID: 1-255

Port numbers: Port 8443 is already in use by system

(up to 8 port numbers, separated by commas)

- ☒ Redirect based on destination port
- ☐ Redirect based on source port (return path)

For IP spoofing, define two services, one based on destination port and another based on source port (return path).

- ☒ Load balance based on server address
- ☐ Load balance based on client address

Applies only if more than one Web Security Appliance is in use.

Router IP Addresses:

Enter either IPv4 or IPv6 addresses; IP address families may not be combined within a single service profile. Separate multiple entries with one break or commas.

Router Security: ☐ Enable Security for Service

Passwords:

The password must be between 1 and 7 characters long.

Confirm Passwords:

> Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

Copyright © www.ine.com



Here is where we can add additional WCCP Service Groups, specifying additional protocols for which we desire the router to redirect to the WSA.



Introducing Cisco Cloud Web Security



Copyright © www.ine.com

Topic Overview

- ▶ Cisco Cloud Web Security Introduction
- ▶ CWS Portal
- ▶ Redirecting Traffic To CWS
- ▶ CWS Towers

Cisco CWS

- ▶ Cloud Web Security provides similar benefits to implementing your own Cisco WSA device, however:
 - ▶ Web traffic redirected to servers hosted by Cisco located in the Cloud
 - ▶ Onsite devices (such as WSA, ISR routers, ASA firewalls, etc) must be configured to redirect web traffic to CWS service
 - ▶ Software components called “Connectors” are used to implement redirection
- ▶ CWS service provides administrative portal through which you can customize your service.

Copyright © www.ine.com



One of the downsides of using the CWS service is you have to account for the fact that there may be times when this service is unreachable...either due to service downtimes (which should be incredibly rare) or internet conditions preventing IP reachability.

-

In these situations you (the administrator) have a choice as to what you want to do with your web requests. You can either configure your device (ASA, WSA, Router, etc) to block-all traffic...or to allow-all traffic.

Cisco CWS Portal



The image shows the Cisco Cloud Web Security (CWS) login portal. It features a light blue background with a decorative graphic of vertical bars in various shades of blue and green on the left. In the center, there is a small globe icon above the text "Cisco Cloud Web Security". Below this, there are two input fields for "Username" and "Password", followed by a blue "Login" button. A link for "Forgotten your password?" is located below the login button. At the bottom left, there is a copyright notice: "© 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries." The Cisco logo is at the bottom right.

© 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries.

Copyright © www.ine.com



Here is an example of the initial login page for accessing the CWS portal.

Cisco CWS Portal

The screenshot displays the Cisco Cloud Web Security (CWS) Portal interface. The top navigation bar includes links for Home, Dashboard, Web Virus, Spyware, Web Filtering, Admin, and Reports. The main content area is titled 'Manage Policy' and shows a table of rules for web filtering. The table has columns for #, Move, Rules, Groups/Users/IPs, Filter, Schedule, Action, Active, Edit, Exceptions, and Delete. Two rules are listed: Rule 1 is 'medium-allow' for 'Anyone' with a 'medium-allow' filter and 'anytime' schedule, set to 'Allow' and active. Rule 2 is 'medium-block' for 'Anyone' with a 'medium-block' filter and 'anytime' schedule, set to 'Block' and active. The interface also includes a 'Manage Policy' button and a 'Create Rule' button.

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Exceptions	Delete
1	↓	medium-allow	Anyone	"medium-allow"	"anytime"	Allow	✓	[P]		[X]
2	↑	medium-block	Anyone	"medium-block"	"anytime"	Block	✓	[P]	✓	[X]

Copyright © www.ine.com



Here is an example of the page within the CWS portal where you would setup web filtering.

Redirecting Traffic To CWS

- ▶ HTTP and HTTPS traffic is redirected to Cisco Cloud Web Security service.
- ▶ All traffic is given additional HTTP headers, applied by Connector software
 - ▶ Cisco Cloud Web Security uses these headers to obtain information about customer deployments, including information about the user who had originally made the client request and the device that sent the request.
 - ▶ For security purposes, the information in the headers is encrypted and then hexadecimal encoded.

Copyright © www.ine.com



More information than any CCNA Security candidate would ever need to know, but if you're curious;

The ISR adds the following CWS HTTP headers:

----X-ScanSafe—This contains a session key that is encrypted using a CWS public key (embedded in the ISR operating system).

----X-ScanSafe-Data—This contains the data CWS needs. It is encrypted with the session key from the X-CWS header.

CWS Towers

- ▶ Cisco Cloud Web Security servers are called, “Towers”.
- ▶ Part of your initial implementation would be to select an appropriate license size, and tower location(s).
- ▶ Tower locations include:
 - ▶ Sydney
 - ▶ Dallas
 - ▶ Frankfurt
 - ▶ Chicago
 - ▶ Secaucus
 - ▶ London
 - ▶ ...and many more

The screenshot shows the 'Edit Cloud Connector Settings' dialog box. The 'Server Address' field is highlighted with a red box and contains the text 'proxy001.cws-400.cisco.com'. Below it, the 'Failure Handling' section shows 'Connect directly' selected. The 'Cloud Web Security Authorization Scheme' section shows 'Send authorization key information with transaction' selected. The 'Authorization Key' field is empty. At the bottom right, the 'Submit' button is highlighted with a red box.

Copyright © www.ine.com



Here you see a screenshot of where you would provide the FQDN of the tower location you wish to use.

-
You purchase CWS licenses based on the number of concurrent internet users you expect to have. “Concurrent users” is defined by Cisco as roughly 15% of your total employee count.



Cisco CWS Connectors



Copyright © www.ine.com

Topic Overview

- ▶ What Are Connectors?
- ▶ ASA Connector
- ▶ ISR G2 Connector
- ▶ WSA Connector
- ▶ AnyConnect Connector

What Are Connectors?

- ▶ Web traffic is redirected from Web Clients to the Cisco CWS service through the use of “Connectors”.
- ▶ Cloud connectors are software components embedded in, hosted on, or integrated with platforms in order to enable or enhance a cloud service.
 - ▶ In other words, if there is no “connector” available for a certain platform, that simply means that platform has no capability of redirecting web traffic to Cisco CWS.

Copyright © www.ine.com



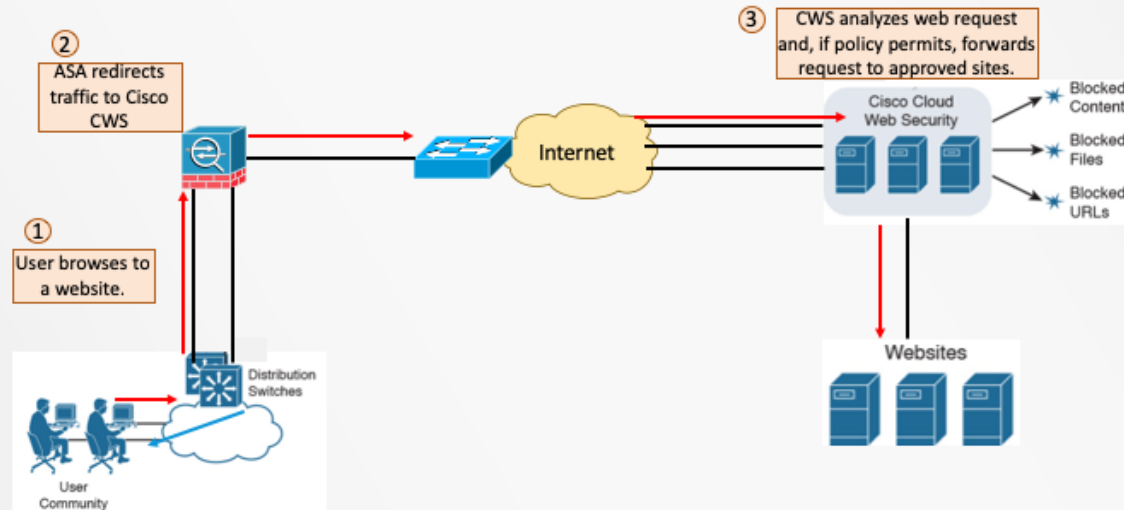
A cloud connector is not some special module or license you have to download. It is code embedded into your existing software that either gives you access to specific CLI commands with which you can connect to the CWS service (either IOS, AnySync or ASA OS commands) or gives you access to specific parts of a GUI that provide this functionality.

If a device is not advertised as having a “Connector” it simply means that device doesn’t have (built into its software) the appropriate code with which to connect to the CWS service.

Available CWS Connectors

- ▷ ASA/ASAv Connector
- ▷ ISR G2 Connector
- ▷ Web Security Appliance (WSA) Connector
- ▷ Cisco AnyConnect Secure Mobility Client with the Web Security Module

Cisco CWS ASA/ASAv Connector

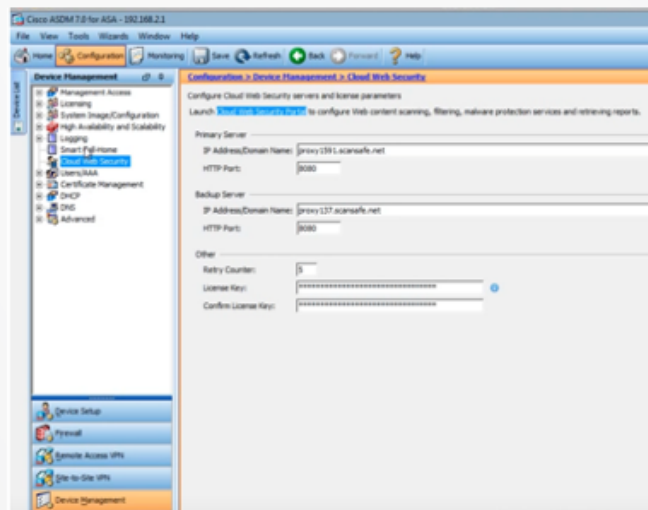


Copyright © www.ine.com



Within the Cisco ASA, you simply need to define the CWS IP Address/Domain name, port number (which is TCP 8080 by default) and License Key. Then, as if you were configuring QoS, you classify the traffic to be redirected by the ASA.

CWS ASA/ASAv Connector

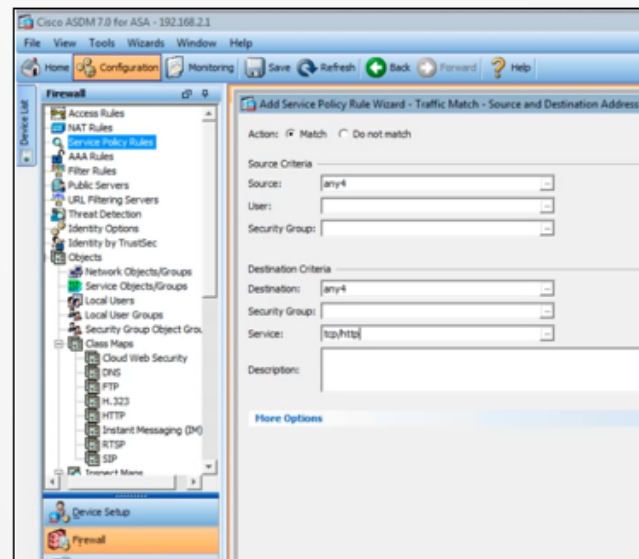


Copyright © www.ine.com



Here are you providing your ASA the necessary information so it knows how to reach the CWS service.

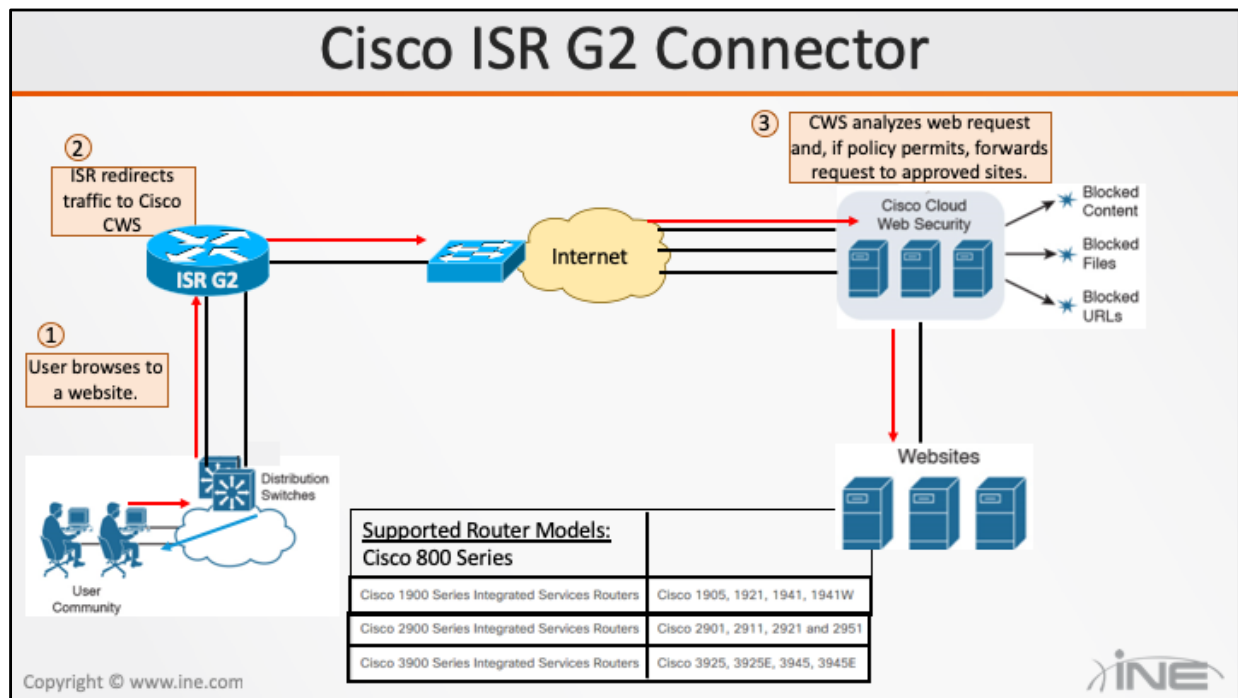
CWS ASA/ASAv Connector



Copyright © www.ine.com



Here are you are classifying all IPv4 TCP HTTP traffic...which will later be tied into a CWS "Inspect Map". For more information watch: <https://www.youtube.com/watch?v=AKiJHyv0EnQ>



A device (such as an ISR router) that forwards web traffic to Cisco Cloud Web Security proxy servers includes additional HTTP headers in each HTTP and HTTPS request. Cisco Cloud Web Security uses these headers to obtain information about customer deployments, including information about the user who had originally made the client request and the device that sent the request. For security purposes, the information in the headers is encrypted and then hexadecimal encoded.

- So one could say that redirected traffic is HTTP/HTTPS traffic that is tunneled inside of additional HTTP headers.

- For more information see: https://www.cisco.com/c/en/us/products/collateral/security/router-security/data_sheet_c78-655324.html

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_cws/configuration/15-mt/sec-data-cws-15-mt-book/scansafe-web-sec.html

CWS ISR G2 Connector

1

Redirect web traffic

```
parameter-map type content-scan global
server scansafe primary ipv4 <primary tower ip> port http 8080 https 8080
server scansafe secondary ipv4 <secondary tower ip> port http 8080 https 8080
license 0 <license key generated above>
source interface GigabitEthernet0/1
timeout server 30
server scansafe on-failure block-all

interface GigabitEthernet0/1
cws out
```

2

Configure ACL whitelisting – By Host

```
parameter-map type regex allowed_hosts
pattern *.cisco.com
cws whitelisting
whitelist header host regex allowed_hosts
```

Notice the command in step-1 of “server scansafe on-failure block-all”. This tells the router that if reachability to the CWS service is down, to block all outgoing web requests from clients. An alternative keyword you could select would be “allow-all”. It really boils down to your personal preference as the network administrator.

CWS ISR G2 Connector

3

Configuring LDAP Server

```
aaa new-model
aaa group server ldap scansafe
server ss-ldap
ldap server ss-ldap
ipv4 <ldap server ip>
transport port 3268
bind authenticate root-dn "<service account distinguished name>" password
<server account password>
base-dn "<search base distinguished name>"
search-filter user-object-type user
authentication bind-first
```

4

Configure user identity

```
aaa authentication login ss-aaa group scansafe
aaa authorization network ss-aaa group scansafe
aaa accounting network ss-aaa none
ip admission virtual-ip 1.1.1.1 virtual-host proxy
ip admission name ssauth ntlm passive inactivity-time 60
ip admission name ssauth order ntlm
ip admission name ssauth method-list authentication ss-aaa authorization ss-
aaa accounting ss-aaa

interface GigabitEthernet0/0
ip admission ssauth
ip http server
aaa authentication login default none
aaa authorization exec default none
```

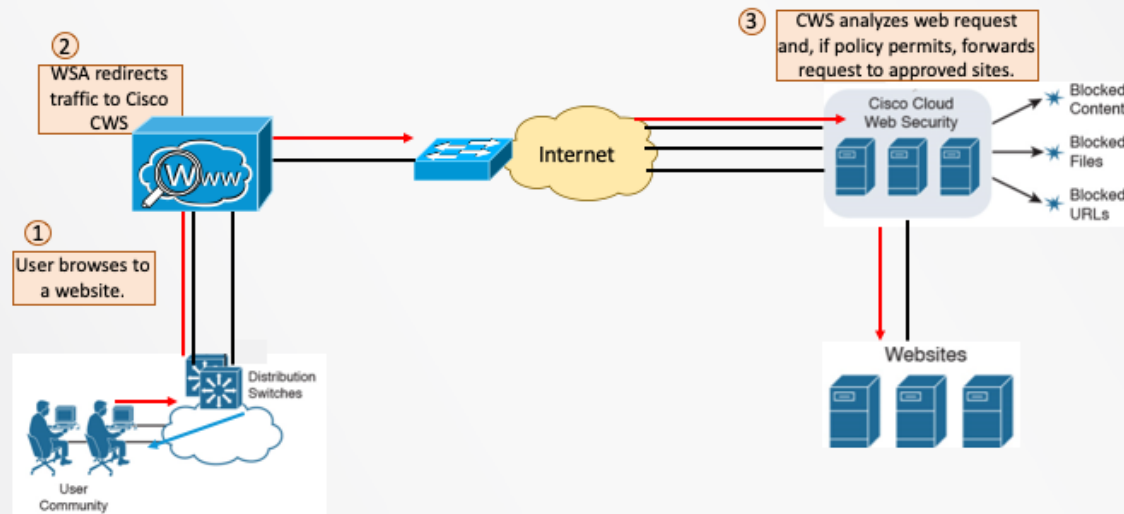
Copyright © www.ine.com



User authentication is an optional step but allows you to enforce unique, per-user policies and keep granular records about user web traffic. In this case, when the user opens their browser and their traffic is redirected to the ISR router, they will see a dialogue box asking for their Username/Password. Once they supply the correct credentials (as authenticated by an LDAP server) they will be allowed to submit web requests. I believe they only have to be authenticated once as a cookie is installed in their browser upon successful authentication. However if they shutdown their browser and re-open it, they'd have to authenticate again prior to doing any web lookups.

Configuration steps for the WSA connector imply that user authentication is optional.

Cisco WSA Connector



Copyright © www.ine.com



CWS WSA Connector

1. Start **2. Network** 3. Security

System Settings

Default System Hostname:
e.g. proxy.company.com

DNS Server(s): ☐ Use the Internet's Root DNS Servers
☒ Use these DNS Servers:

(optional)
 (optional)
 (optional)

NTP Server:

Time Zone: Region: GMT Offset:

Country: GMT:

Time Zone / GMT Offset:

Appliance Mode

Appliance Mode of Operation ☐ Standard
This appliance will be used for on-premise policy enforcement (Standard Web Security Appliance installation).

☒ Cloud Web Security Connector
This appliance will be used primarily to direct traffic to Cisco Cloud Web Security (Cloud Web Security Connector installation).

CWS WSA Connector

 Cisco IronPort S650
Web Security Appliance

1. Start **2. Network** 3. Review

Cloud Web Security Connector Settings

Cloud Web Security Proxy Servers: ?

Server Address
proxy1731.scansafe.net
proxy193.scansafe.net

hostname or IP address

Failure Handling: Specify how to handle requests if all specified Cloud Web Security Proxy servers fail.

☒ Connect directly

☐ Drop requests

Cloud Web Security Authorization Scheme:

☐ Authorize transaction based on IP address

☒ Send authorization key information with transaction

Authorization Key: 186FDF; :09AD48

AnyConnect CWS Connector

- ▶ **Built into Cisco AnyConnect 3.1 client**
 - ▶ Utilizes built-in Cloud Connector for Cisco CWS service
- ▶ **Allows for split-tunneling**
 - ▶ Intranet traffic goes through normal SSL/IPsec VPN back to corporate HQ.
 - ▶ Internet traffic redirected to CWS service.
- ▶ **Only the Cisco AnyConnect 3.1 client for Windows and Mac OS X include support for the Cisco AnyConnect CWS Module. Other types of mobile devices must connect to their primary site RAVPN firewall and secure their web traffic with resources located at the primary site.**

Copyright © www.ine.com



With regards to using the Cisco AnyConnect connector, a feature built into the Cisco AnyConnect 3.1 client is the “Cloud connector for Cisco Cloud Web Security (CWS) service”. A network admin would first enable this service/module which then allows an organization to use a split-tunneling approach on each remote laptop using AnyConnect. Only traffic destined to the organization is sent to the central site. All web traffic to the Internet from remote-access VPN users accesses the Internet through the cloud-based CWS service

-

Not supported on iPhones and iPads. Only works with AnyConnect software designed for Laptops and PCs.