Cloud Web Security:
Traffic Redirection Methods

May 2017

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Overview

This document provides guidance on selecting a mechanism for redirecting web traffic to Cisco Cloud Web Security (CWS).

The traffic redirection methods currently in use by customers are:

- ASA platforms
- ISR platforms
- CWS Connector
- WSA Connector
- Direct-To-Tower methods (Hosted PAC files, third-party proxies, explicit browser configuration)
- AnyConnect

Selecting a Method to Redirect Web Traffic

The process of selecting a traffic redirection method is captured in Figure 1 below, and is applicable to most customer environments.

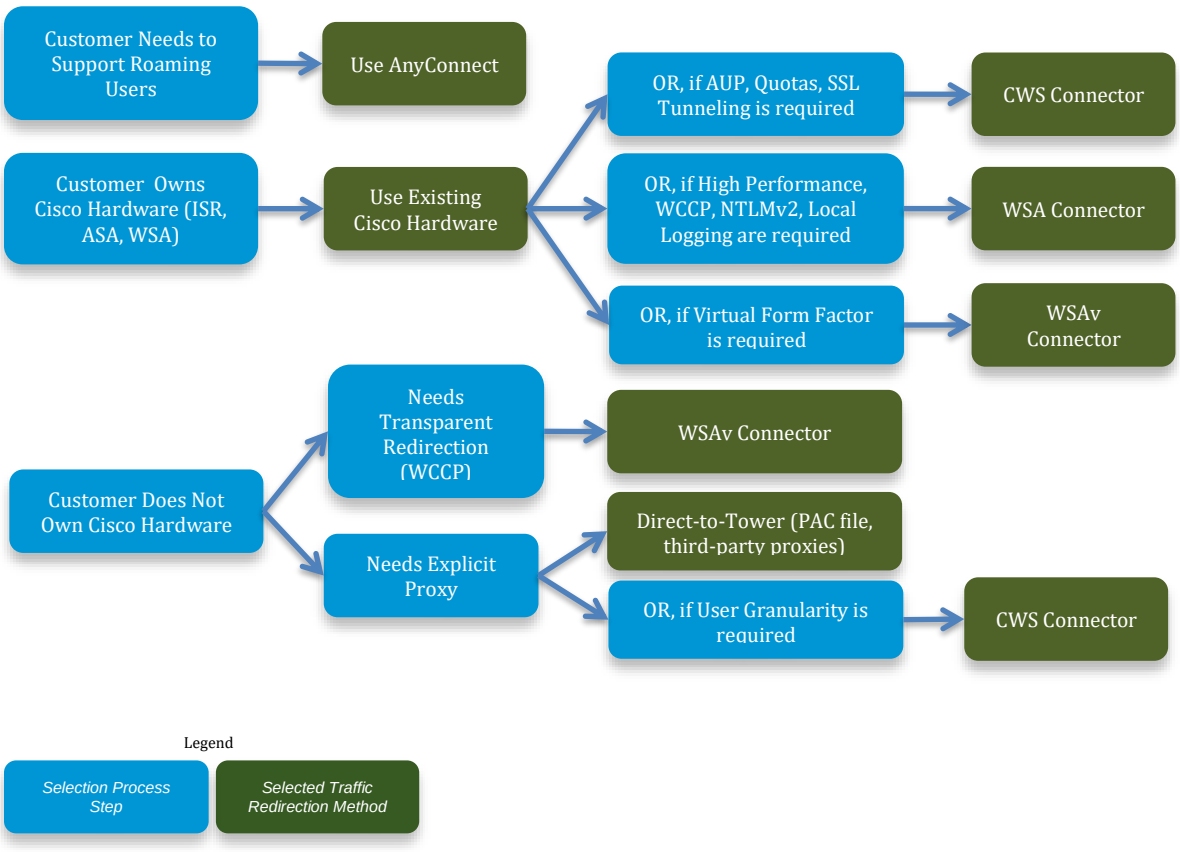

Figure 1: Traffic redirection methods

Customers who own Cisco hardware (ISR, ASA, or WSA) are encouraged to leverage the integrated traffic redirection capabilities of their platforms. For all other environments, the choice of traffic redirection is between the CWS Connector, the WSAv Connector or Direct-To-Tower methods.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

When To Redirect Traffic Using Direct-To-Tower Methods

Customers who do not have an ASA or ISR in their environment should send traffic directly using PAC files, third-party proxies or explicit browser settings. Direct-To-Tower methods can be used with EasyID and SAML to capture user identity.

Choosing between the CWS Connector and the WSAv Connector

The selection process between these two options depends primarily on whether customers want to redirect traffic transparently to CWS. Figure 2 outlines the selection process, based on the two most important criteria: proxy type and sizing requirements.

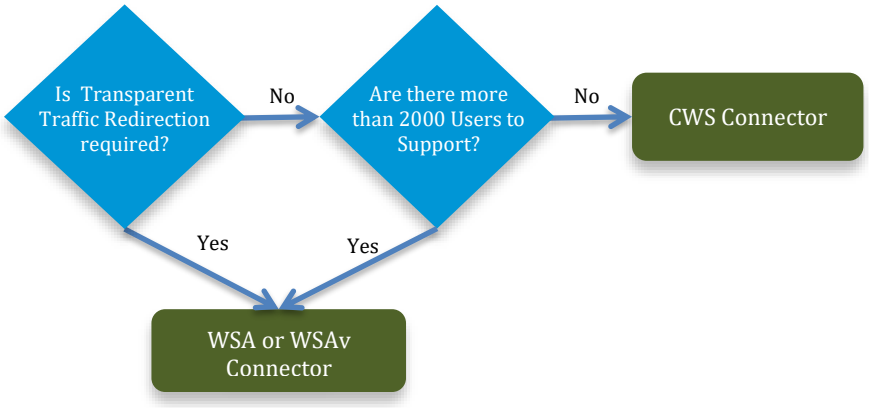

Figure 2: Choosing between CWS and WSAv Connectors

CWS Features Supported By Traffic Redirection Options

Table 1 below lists the Cloud Web Security features supported when using a specific traffic redirection option.

CWS Feature	ASA Connector	ISR-G2 Connector	ISR-4K Connector	WSA Connector	Native Connector	Hosted PAC File	AnyConnect	Mobile Browser
HTTPS Inspection (MITM) [1]	Supported across all redirection options							
Web Filtering Exceptions	Supported across all redirection options							
URL Categorization	Supported across all redirection options							
Application Visibility and	Supported across all redirection options							
URL Dynamic Classification	Supported across all redirection options							
Customizable Notifications	Supported across all redirection options							
Outbreak Intelligence	Supported across all redirection options							
Cloud Whitelisting	No	Yes	Yes	No	No	No	Yes	Yes
AUP [2]	No	No	No	No	Yes	No	No	Yes
Quotas [3]	No	No	No	No	Yes	No	No	No

Table 1: Supported CWS Features

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Feature Comparison Across Traffic Redirection Options For CWS

All traffic redirection options listed below have the ability to redirect web traffic (port 80 and 443) and forward authenticated user details to CWS. Table 2 lists the capabilities supported by each traffic redirection option.

CWS Feature	ASA Connector	ISR-G2 Connector	ISR-4K Connector	WSA Connector	CWS Connector	Hosted PAC File	AnyConnect	Mobile Browser
	Redirection Capabilities							
Traffic Redirection Method	Transparent	Transparent	Transparent (via Secure Tunnel)	Transparent (WCCP) / Explicit	Explicit	Explicit	Transparent	Transparent
How Devices Authenticate to Cloud	License Key [4]	License Key [4]	License Key [4]	License Key [4]	License Key [4] and Egress IP	Egress IP	License Key [4]	License Key [4]
Tower Failover [5]	Failover is determined by lost connection not slow connection Connection to the towers is checked at regular intervals and failover to another tower occurs on the platform if tower does not return a response					Via proxy PAC file	Available when configured with Detect Closest Tower (DCT)	Available when configured with Detect Closest Tower (DCT)
SSL Tunneling [6]	No	No	GRE over IPsec	No	Yes	No	Yes (default)	No
Whitelisting (Exceptions) [7] Options	IP, IP Ranges	IP, IP Ranges, URL Host (with wildcard), User Agent	IP, IP Ranges, URL Host (with wildcard)	IP/CIDR, FQDN, URL (with wildcard), User Agent	IP, IP Ranges, URL Host (with wildcard), User Agent	IP, IP Ranges, URL Host (with wildcard), User Agent	IP, IP Ranges, Host	IP, IP Ranges, URL Host (with wildcard)
	User Authentication Mechanisms							
Mechanism	IDFW	ISR AAA Services	Future release [9]	LDAP, NTLM, CDA	Proxy NTLM	N/A	GP result API - Windows	N/A
Additional Options [8]	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML
Transparent	Yes	Yes	Future release [9]	Yes (NTLM, CDA)	Yes	No	Yes	Yes
Supported Browsers	IE, FF, Safari, Chrome	IE, FF, Safari, Chrome	Future release [9]	IE, FF, Chrome	IE,FF, Chrome	N/A	IE, FF, Safari, Chrome	N/A
Supported OS	Windows / OS X	Windows	Future release [9]	Windows	Windows	N/A	Windows / OS X	iOS / Android
Non transparent	Yes	Yes	Future release [9]	Yes	Yes	Yes	No	Yes
Supported Browsers	All	All	Future release [9]	All	All	All	N/A	N/A
Supported OS	Windows / OS X / iOS devices	Windows / OS X / iOS devices	Future release [9]	Windows / OS X / iOS	Windows / OS X / iOS devices	Windows / OS X / iOS devices	N/A	iOS / Android
Supported Protocols	LDAP and Radius (via CDA)	NTLM (v1, v2), LDAP, TACACS and Radius	Future release [9]	NTLM, Basic (LDAP)	NTLM (v1)	N/A	NTLM - Windows API	N/A
Supported Versions	9.0 and above	ISR G2, 15.3(3) M3	IOS XE 3.16.x [10]	8.x	Any	N/A	3.0 and above	N/A

Table 2: Traffic Redirection Options Supported Feature Matrix

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Additional details:

1. HTTPS inspection is an optional feature for scanning of HTTPS traffic.
2. Acceptable Use Policy (AUP) is supported only with the CWS Connector, which tracks if/when users last agreed to an AUP.
3. Quotas are supported only with the CWS Connector, which tracks browsing usage.
4. A Company/Group key is always used with ASA, ISR, and AnyConnect. This is optional with CWS Connectors, and can be replaced by scanning IPs specified in ScanCenter.
5. All connectors provide the ability to configure a primary and a secondary proxy.
6. SSL Tunneling is a feature that encrypts all communications between the Connector and the cloud infrastructure via an SSL tunnel.
7. Whitelisting is configured and enforced at the Connector level to prevent certain traffic from being redirected to CWS (and hence bypass scanning). This feature can also be configured through a PAC file when using explicit proxy settings.
8. Additional options denote authentication mechanisms that can be used instead of the platform's built-in authentication mechanisms. Note that in some cases, SAML authentication may not be transparent to the end user, prompting them to authenticate with their credentials.
9. Active auth on ISR4K is expected to be available only in **Controlled Availability** from v3.16.6.
10. CWS connector on ISR4K is available only on 3.16.x releases, and not on Polaris 16.x builds.

Frequently Asked Questions

How do I determine if I need a high performance solution?

Each configuration guide listed in Table 3 provides guidelines on the maximum number of users that the specific traffic redirection method supports. For environments that exceed these limits, customers may consider using additional devices for traffic redirection, or using Direct-To-Tower redirection in conjunction with user identity obtained through EasyID or SAML.

How do customers secure remote user web traffic*?*

For users who are remote and operate outside the boundaries of the corporate network, use the AnyConnect client to redirect traffic to CWS. For details on configuring AnyConnect, please refer to: http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Dec2013/CVD-CloudWebSecurityUsingCiscoAnyConnectDesignGuide-DEC13.pdf

Configuration Reference Information

For detailed information on how to configure a traffic redirection option, please refer to the relevant documentation listed in Table 3:

Redirection Method	Reference
ASA	ASA Connector Quick Configuration Guide: http://dcg.cisco.com/go/5v
ISR	CWS Configuration Guide: http://dcg.cisco.com/go/5w
CWS Connector	Connector Administrator Guide: http://dcg.cisco.com/go/5x
WSA / WSAv Connector	Cisco AsyncOS for Web User Guide: http://dcg.cisco.com/go/5y
AnyConnect	CWS Using AnyConnect – Technology Design Guide: http://dcg.cisco.com/go/5z

Table 3: Reference and Configuration Guides

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

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)

Printed in USA

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.