



Feature comparison across traffic redirection options for Cisco Cloud Web Security

The table below lists the different traffic redirection options when deploying Cisco Cloud Web Security (CWS). This includes details such as authentication mechanisms and features supported on individual platforms. Please refer to this table before transitioning from your existing deployment option.

All platforms listed have the capability to redirect traffic (port 80 and 443) and forward authenticated user details to Cisco Cloud WebSecurity. The supported features differ depending on which platform is used to connect to CWS					
	ASA Connector	ISR Connector	Native Connector	Hosted PAC	AnyConnect
Cloud Web Security features supported whilst using any platform					
HTTPS Inspection (MITM) ¹	All platforms				
Web Filtering Exceptions	All platforms				
URL Categorization	All platforms				
Application Visibility and Control feature	All platforms				
URL Dynamic Classification	All platforms				
Customizable Notifications	All platforms				
Outbreak Intelligence (Zero Day Malware)	All platforms				
Outbound Content Control	All platforms				
AUP ²	No	No	Yes	No	No
Quotas ³	No	No	Yes	No	No
Redirection Capabilities					
Supported user redirection method	Transparent	Transparent	Explicit	Explicit	Transparent
How devices authenticate to cloud	License Key ⁴	License Key ⁴	License Key ⁴ and Egress IP	Egress IP	License Key ⁴
Tower Failover ⁵	Failover is determined by lost connection not slow connection - Connection to the towers is checked at regular interval and failover to another tower occurs on the platform if tower does not return a response			Via proxy PAC file	Available in version 3.1 when configured with Detect Closest Tower (DCT)
SSL Tunneling ⁶	No	No	Yes	No	Yes (default)
Whitelisting (Exceptions) ⁷ options	IP, IP Ranges	IP, IP Ranges, URL Host (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

	ASA Connector	ISR Connector	Native Connector	Explicit Proxy	AnyConnect
Authentication details					
Mechanism	IDFW	ISR AAA Services	Proxy NTLM	N/A	GP result API - Windows
Additional options ⁸	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML
Transparent	Yes	Yes	Yes	No	Yes
Supported browsers	IE, FF, Safari, Chrome	IE, FF, Chrome	IE, FF	N/A	IE, FF, Safari, Chrome
Supported Operating Systems	Windows / OS X	Windows	Windows	N/A	Windows / OS X
Non transparent	Yes	Yes	Yes	Yes	No
Supported browsers	All	All	All	All	N/A
Supported Operating Systems	Windows / OS X / iOS devices	Windows / OS X / iOS devices	Windows / OS X / iOS devices	Windows / OS X / iOS devices	N/A
Supported protocols	NTLM (v1, v2), LDAP, Kerberos, TACACS and Radius	NTLM (v1, v2), LDAP, TACACS and Radius	NTLM (v1)	LDAP	NTLM - Windows API
Version that supports CWS Integration	9.0 above	ISR G2, 15.2 MT	Any	N/A	3.0 above

Additional details:

1. HTTPS inspection is an optional feature (no additional cost) for scanning of HTTPS traffic.
2. Acceptable Use Policy (AUP) is available only with Native Connector which controls this by keeping track of when/if users last agreed to this. This is not done in the cloud, or by other Connectors
3. Quotas are available only with Native Connector which controls this by keeping track of browsing usage. This is not done in the cloud, or by other Connectors
4. A company/Group key is always used with ASA, ISR, and AnyConnect. This is optional with Native Connectors, and can be skipped if scanning IPs are defined in ScanCenter
5. All connectors have 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 at Connector level to whitelist certain traffic from being redirected to CWS. This can 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



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)