



Security Configuration Guide: Cloud Web Security, Cisco IOS XE Release 3S

Cisco 4000 Series ISR Cloud Web Security Connector	2
Prerequisites for Cloud Web Security Tunneling	2
Restrictions for Cloud Web Security Tunneling	3
Information About Cloud Web Security Tunneling	4
How to Configure Cloud Web Security Tunneling	9
Verifying the Cloud Web Security Tunneling Configuration	15
Additional References for Cloud Web Security Tunneling	20
Feature Information for Cloud Web Security Tunneling	21

Revised: November 12, 2019

Cisco 4000 Series ISR Cloud Web Security Connector

Tunnel connector for Cisco Cloud Web Security is a cloud-delivered web security solution. Cisco Cloud Web Security controls access to websites and specific content in web pages and applications. Administrators can set and enforce web use policies across the network for applications, websites, and webpage content.

In Cisco 4000 Series Integrated Services Routers, Cisco Cloud Web Security is delivered through a tunneling method. HTTP and secure HTTP (HTTPS) traffic from ISRs to Cloud Web Security tower is transported through generic routing encapsulation (GRE) over IPsec tunnels.

This module describes the Cloud Web Security Tunneling feature and explains how to configure it on Cisco 4000 Series Integrated Services Routers.

Prerequisites for Cloud Web Security Tunneling

- Cisco 4000 Series Integrated Services Routers must be configured with security K9 license.
- Cloud Web Security subscription license must be configured on the device.
- You can import the Certificate Authority (CA) for tunnel authentication certificate into Cisco ISR 4000 Series Integrated Services Router.

```
Device(config)# crypto pki trustpoint cws-trustpoint
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# exit
Device(config)# crypto pki authenticate cws-trustpoint
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
----BEGIN CERTIFICATE-----
MIIGxDCCBKygAwIBAgIUdRcWd4PQQ361VsNX1G5FY7jr06wwDQYJKoZIhvcNAQEL
BQAwRTElMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFFlbn1Zb3ZGlzIEExpbWl0ZWQxGzAZ
BgNVBAMTElF1b1Zb3ZGlzIFJvb3QgQ0EgMjAeFw0xMzEyMTcxNDI1MTBaFw0yMzEy
MTcxNDI1MTBaMF4xGzAxBgNVBAYTA1VTMTAwLgYDVQQKEydIeWRyYW50SUQgKEF2
YWxhbmNoZSBDbG91ZCBDb3Jwb3JhdGlvbikxHTAbBgNVBAMTFEh5ZHZhbnRJRjCBT
U0wgSUNBIEcyMlICiANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA9p1ZOA9+
H+tgdlN+STF7bdOxvnoERYyjo8ZbKumzigNePSwbQYVWuso76GI843yjaX2rhn0+
Jt0NVJM41jVctf9gwacVduR7CEi0qJgpAUJyZUuB9IpFWF1Kz1403Leh6URuRZ43
RzHaRmNtzkxttGBuOtAg+ilOuwiGAo9VQLgdONlqQFcrbp97/f08ZiQiPrbhLxCZ
fXkYi3mktZVRFXKG62FHAuH1sLDXCKba3avDcUR7yK4ZXCmp6k114UKa8JHOHPE
NYyr0R6oHELOGZMoxlnQcFwuYMX9sJdAUU/9SQVXyA6u6YtxlpZiC8qhXm1IE00T
Q9+q5ppffSUDMC4V/5If5A6snKVP78M8qd/RMVswcJmUMEnov+wykCbDLD+IREM
A57XX+HojN+8XFTL9Jwge3z3ZlMwL7E54W3ci7f6cx05DVwoKxkdk2jRIg37oqS1
SU3z/bA9UXjHcTl/6BoLho2p9rWm6oljANPeQuLHyGJ3hc19N8nDo2IATp70klGP
kd1qhIgrdkki7gBpanMOK98hKMpdQgs+NY4DkaMJqfrHzWR/CYkdyUCivFaepaFS
K78+jVu1oCMOFOnucPXL2fQa3VQn+69+7mA324frjwZj9NzrHjd0a5UP7waPpd9W
2jz0j4b+g+l+XU1SQ+9DWiuZtvFDW++k0BMCAwEAAoCAZEwgGnMBIGA1UdEwEB
/wQIMAYBAf8CAQAwEAYDVR0gBHEwbzAIBgZngQwBAGewCAYGZ4EMAQICMA4GDCsG
AQQBvlgAAmQBAJBjBgwrBgEEAb5YAAOHBAAwOTA3BggrBgEFBQcCARYraHR0cDov
L3d3dy5oeWRyYW50aWYyZ29tL3N1cHBvcnQvcmlkL3NpdG9yeTBvBggrBgEFBQcC
AQRmMGQwKgYIKwYBBQUHMAAGHmh0dHA6Ly9vY3NwLnF1b3Zb3ZGlzZ2xvYmFsLnNv
bTA2BggrBgEFBQcCwAoYqAHR0cDovL3RydXN0LnF1b3Zb3ZGlzZ2xvYmFsLnNvbS9x
dnJjYTIuY3J0MA4GA1UdDwEB/wQEAwIBBjAFBgNVHSMGDAWgBQahGK8SEwzJQTU
7tD2A8QZRTGuazA5BgNVHR8EMjAwMC6gLKAqhiodHRwOi8vY3JsLnF1b3Zb3ZGlz
Z2xvYmFsLnNvbS9xdnJjYTIuY3J0MA4GA1UdDgQWBBSYarYtLr+nqp/299YJr9WL
V/mKtZANBgkqhkiG9w0BAQsFAAOCAgEAlraik8EDDUkpAnIOajO9/r4dpj/Zry76
```

```

6SH1oYPo7eTGzpDanPMeGmuSmwdjUkFUPALuWwkaDERfz9xdyFL3N8CRg9mQhdtT
3aWQUv/iYXULXT87EgL3b8zzf8fhTS7r654m9WM2W7pFqfimx9qAlFe9XcV1ZrUu
9hph+/MfWMrUju+VPL5U7hZvUpG66mS3BaN15rsXv2+Vw6kQsQC/82iJLHvtYVL/
LwbNio18CsinDeyRE0J9w1YDqzcg5rhD0rtX4JEmBzq8yBRvHIB/023o/vIO5oxh
83Hic/2Xgwksf1DKS3/z5nTzhsUIpCpwkN6nHp6gmA8JBXoU1KQz4eYHJCq/ZyC+
BuY2vHpNx6101J5dmy7ps7J7d6mZXzguP3DQN84hjtFWJPqdf+/9RgLriXeFTqwe
snxbk2FsPhwxhiNOH98GSZVvG02v10uHLVaf9B+puYpoUiEggm1WG5mWW1PxHstu
Ew9jBMcJ6wjQc8He9rSUMrhBr0HyhckdC99RgEvpcZpV2XL4nPPrTI2ki/c9xQb9
kmhVGonSXy5aP+hDC+Ht+bxmc4wN5x+vB02hak8Hh8jIUSTRxOsRfJozU0R9ysyP
EZAHFZ3Zivg2BaD4tOISO8/T2FDjG7PNUv0tgPAOKw2t94B+1evrSUhqJDU0Wf9c
9vkaKoPvX4w=
----END CERTIFICATE----

```

Trustpoint 'cws-trustpoint' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:

```

Fingerprint MD5: 1135E326 56E5AADF 53A4DD32 C8D5590F
Fingerprint SHA1: AC4A728B 4DFC3560 1FA34B92 2422A42C 253F756C

```

```

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

```

- Cisco devices must use Cisco IOS Release 15.5(3)S1 or later image version

Restrictions for Cloud Web Security Tunneling

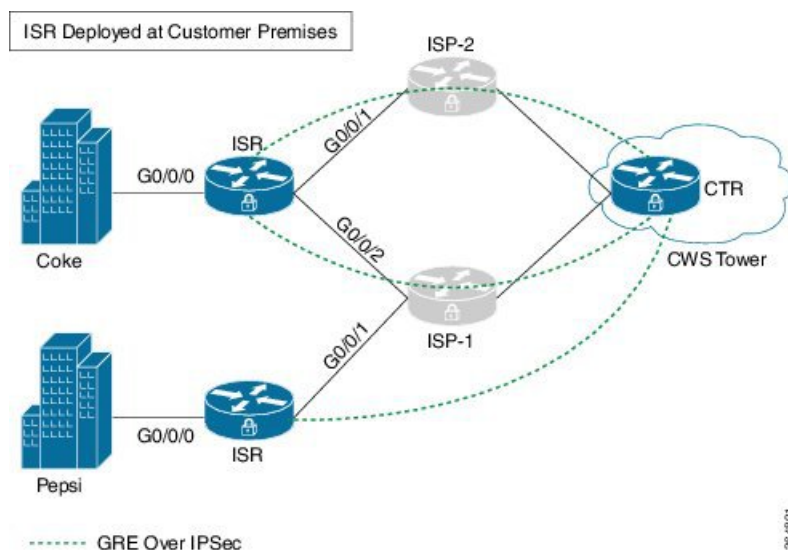
- Zone-based firewall, VRF, and other features configured on the "cws-tunnel out" interface must be manually configured on all the CWS tunnel interfaces.
- IPv6 is not supported.
- IP Admission feature is supported only within the CWS solution.
- If the **cws-tunnel out** command is disabled, the imported CA certificate is automatically deleted from the router (Cisco 4000 Series ISR). The certificate must be imported again, while reconfiguring the **cws-tunnel out** command on the interface.
- Only one access control list (ACL) can be configured through the CLI for whitelisting.
- Object-group ACLs are not supported for ACL based whitelisting and redirect list configuration.
- Any pre-existing tunnel is overwritten when the Cloud Web Security tunnel is configured with same tunnel number.
- The **cws-tunnel out** command can be configured up to a maximum of 2 WAN interfaces.
- DNS resolution happens only through Cisco ISR 4000 series for domain based whitelisting functionality.
- If DNS redirection (such as OpenDNS) is used then regular expression pattern matching using the DNS agent will fail.
- Cisco ISR 4000 series can accept maximum of 64 DNS patterns. Each pattern length can be not more than 100 bytes.
- HSECK9 license is required for a feature to have full crypto functionality. Without this license, only 225 secure tunnels and 85 Mbps of crypto bandwidth would be available. The HSECK9 license allows features in the securityk9 technology package to use the maximum number of secure tunnels and crypto bandwidth. To enable the HSECK9 license, purchase the FL-44-HSEC-K9 license from Cisco and install it using the **license install license-files** command. For more information on obtaining and installing feature licenses, see *Configuring the Cisco IOS Software Activation* feature module.

Information About Cloud Web Security Tunneling

Cloud Web Security Tunneling Overview

Cloud Web Security Tunneling transparently redirects web traffic to the cloud for inspection. Tunnel mode Cloud Web Security solution proposes a dedicated tunnel to be setup from Cisco 4000 Series Integrated Services Routers to cloud for sending the redirected web traffic. The tunneling connector design uses Cloud Tunnel Relay (CTR) infrastructure on the cloud to transport web traffic.

Figure 1: Cloud Web Security Tunneling



The Cloud Web Security Tunneling feature provides the following functionality:

- Transparent redirection of web traffic.
- Allows bypassing of traffic to the Cloud Web Security tower using access control lists (ACLs) and domain-based whitelisting.
- Exception rules can be managed through ScanCenter
- Supports dual-WAN and virtual routing and forwarding (VRF) instances.

When Cloud Web Security Tunneling is configured, the Cisco 4000 Series Integrated Services Routers sets up a dedicated generic routing encapsulation (GRE) over IPsec tunnel with the Cloud Web Security tower to send web traffic.

Whitelisting in Tunnel Connector for Cisco Cloud Web Security

Cisco ISR 4000 series checks if the packet matches whitelisting rules and determines if the packet should bypass Cloud Web Security redirection or not. Cloud Web Security Tunneling feature on ISR 4000 Series Routers support both access control list (ACL) and domain names-based whitelisting rules.

- ACL-based—Standard and extended ACLs are supported. ACL configured through Cisco web security portal supports either source or destination address/mask, but not both, in a single entry.
- Domain name-based—Fully qualified domain names (FQDNs) and regular expression patterns are supported.

Access Control List Based Whitelisting

ACL whitelist can be configured through the CLI or downloaded from the cloud.

ACL-Based Whitelisting Through CLI

Only one ACL-based whitelist can be configured through the CLI. Standard, extended and named ACL's are supported, but object-group ACL's are not supported.

ACL-Based Whitelisting Through Tower

Whitelisting can be provisioned on tower using URL: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_cws/configuration/15-mt/sec-data-cws-15-mt-book/cws-whitelist-towr-telmtry.html.

Cisco 4000 Series Integrated Services Routers polls the Cloud Web Security tower at intervals through requests to the active tower IP address.

Domain-Based Whitelisting for Cloud Web Security

Domain-based whitelisting allows you to bypass some of the web traffic directly to web-server and helps you to skip the Cisco Web Security scanning. The whitelist rules are in the form of FQDN and/or regular expressions. The whitelist rules can be configured both through CLI and/or downloaded from CWS portal. DNS snooping agent intercepts DNS responses for matching FQDN / regular expression and creates a database of whitelisted IP addresses, which are then used for whitelisting the intended web traffic.



Note Downloaded rules are given priority over CLI configuration rules. Whitelisted rules can be viewed using **show cws-tunnel whitelist** command. Downloaded whitelisting rules from the Cloud Web Security tower are not stored in the running configuration. The default polling interval is 60 minutes (one hour).

Cloud Web Security Tunneling

The tunnel between the Cisco ISR 4000 Series Router and the Cloud Tunneling Relay (CTR) is a generic routing encapsulation (GRE)-over IPsec tunnel.

Cloud Web Security Tunneling is usually configured with primary and secondary tower addresses for failover. When Cloud Web Security Tunneling is configured on the WAN-side physical interface, two tunnel interfaces (per physical interface) are automatically created; one pointing to the primary tower and other to the secondary tower, with physical interface as the source. When you configure **cws-tunnel out tunnel-number** X on the WAN interface, then Cloud Web Security creates tunnel X to the primary tower and tunnel X+1 to the secondary tower.



Note Egress features configured on physical WAN interfaces do not automatically get replicated to tunnel interfaces. For example, VRF and zones must be manually configured on the tunnel interface.

Failover

If the primary Cloud Tunnel Relay (CTR) is down, Cisco ISR 4000 series will try to establish GRE over IPsec tunnel with secondary CTR.

In the event of primary CTR failover, traffic redirection and whitelisting rules download happens through secondary CTR.

When both primary and secondary CTR's are down and fail-open is not configured under Cloud Web Security parameter-map, all HTTP/HTTPS traffic will be dropped. If fail-open CLI is configured, HTTP/HTTPS traffic will be allowed to pass based on routing information.

When primary is up after failover, redirection will happen through primary tunnel.

Dual WAN Interfaces

A connector can have up to a maximum of two WAN interfaces, with each interface going through different links such as 3G/ADSL etc. If there are multiple WAN interfaces, Cloud Web Security can be enabled on a maximum of 2 WAN interfaces. In Dual-wan scenario, Cloud Web Security creates four tunnel interfaces (2 per WAN Interface). User traffic redirection in this case is dependant on routing. If routing points Cloud Web Security to WAN1, Cloud Web Security will use active tunnel (primary or secondary) of that WAN to reach the tower.

For whitelist download, Cloud Web Security selects least active tunnel number among the four tunnel interfaces. For example, if Cloud Web Security dynamically creates tunnel interfaces 100 and 101 on WAN1 and 200 and 201 on WAN2, the order of preference for whitelist download is tunnel 100 (active) > tunnel 101(standby) > tunnel 200 (active) > tunnel 201(standby). If tunnel 100 is down, whitelist download happens via 101. If WAN 1 is down, whitelist download happens over active tunnel of WAN2 (in this case, it is 200).



Note It is recommended to assign lower tunnel number on WAN interface that has better bandwidth.

Cloud Web Security Tunneling Performance Matrix

This table displays the Cloud Web Security tunneling performance:

Table 1: Cloud Web Security Connector Performance Matrix

Platform	Connection Type	Clients	Transactions Per Second	Concurrent Connections	Response Time (ms)	Bandwidth (Mbps)
Cisco 4451 ISR	Tunnel	2975	1960	69500	45	500
Cisco 4321 ISR	Tunnel	475	300	10425	76	76

Cloud Web Security Interaction with Other Features

Cloud Web Security Interaction with Zone-based Firewall:

If a zone is configured on WAN interface where **cws-tunnel out** is configured, the same zone has to be manually applied on the dynamically created Cloud Web Security tunnel interfaces. If a different zone is applied on dynamically generated Cloud Web Security tunnels, make sure to configure the required firewall policy.

If **cws-tunnel out** command is removed and reapplied on WAN interface, the zone information on tunnel interfaces has to be reconfigured. This is due to the fact that all the configuration that was applied on tunnel interfaces gets removed when Cloud Web Security is unconfigured on WAN interface.



Note Configure zones on both primary and secondary tunnel interfaces. This will make sure the traffic is not dropped due to Zone-based firewall after fail-over.

Cloud Web Security Interaction with VRF:

If VRF is configured on WAN interface where **cws-tunnel out** is configured, change the autogenerated Cloud Web Security configuration to the following:

- Add command **match fvr** *name-of-vrf* under dynamically generated Cloud Web Security IKEv2 profile. For example, if WAN interface is configured to be part of VRF ISP, add **match fvr** *ISP* under **cws_ikev2_profile** *<tunnel_number>*.
- Add command **tunnel vrf** *name-of-vrf* and **vrf forwarding** *name-of-vrf* under dynamically generated Cloud Web Security tunnel interface.

If **cws-tunnel out** command is removed and reapplied on WAN interface, the VRF information on Cloud Web Security tunnel interfaces and IKEv2 profile has to be reconfigured.



Note Configure VRF information on both primary and secondary tunnel interfaces. This will make sure the traffic goes through respective VRF after fail-over.

Configuring **vrf forwarding** on the Cloud Web Security tunnel interface would need the IP unnumbered interface to be reapplied.

Cloud Web Security Interaction with WAAS UCS-E:

If WAAS is installed on Cisco ISR 4000 series over UCS-E card, we need to add **cws-tunnel in** command on the ingress interface connected to WAAS UCS-E card.

Redirecting Packets in Cloud Web Security Tunneling

HTTP(S) traffic (and any traffic classified by Port Address Mapping as HTTP(S)) is transparently redirected to CTR by configuring **cws-tunnel in** command on interfaces where client subnet is connected. If the HTTP(S) traffic matches the whitelist configured through CLI or downloaded from tower, the client traffic is not redirected through CTR.

The following information is required to redirect a packet:

- Primary and secondary tunnel: Information about the tunnels associated with each physical egress interface on which the **cws-tunnel out** command is configured.
- Active tunnel information: The active tunnel from among the primary and secondary tunnels.

Each WAN configured with the **cws-tunnel out** command will have 2 tunnel interfaces. The following logic is used to determine the active tunnel for WAN interfaces:

	Primary tunnel	Standby tunnel	Active tunnel
Tunnel status	Up	Standby	Primary
	Down	Up	Standby
	Down	Down	None

Identity Based Policy In Cloud Web Security

Cisco Cloud Web Security allows you to create policy per user. The user can be authenticated using Active Identity functionality on Cisco 4000 Series ISRs. This functionality is used for end-point authentication and authorization. For more details, See the [Configuring NTLM-based Authentication on the Cisco 4000 Series ISR](#) guide.

When the user is authenticated successfully, Cisco 4000 Series ISR learns the various user-groups that the user associated with. This information is passed to Cisco Cloud Web Security so that appropriate policies can be applied to user-traffic.

Cisco Cloud Web Security connector registers with the Active identity to get the user identity information after the user authenticates. Unique Identifier (UID) module in the Cloud Web Security connector receives this identity information and converts it into a 32-bit unique ID (unique in Cisco 4000 Series ISR level). Cisco 4000 Series ISR posts this UID and user identity mapping (UID <-> user name, user groups) to the UID service in the Cisco Cloud Web Security (through REST service).

The following show command displays the UID and the UID Post status for the authenticated clients:

```
Device#show cws-tunnel uid
IP-Address      UID          Expiry Time  Status
192.168.1.3     3232235779  300         201_RECV
```

The following show command displays cumulative statistics for the UID Post Requests sent and Responses received alongwith the UID Post success or failure:

```
Device#show cws-tunnel statistics
Whitelist Download Success 0
Whitelist Download Failed 0
Uid Requests 1
Uid Responses 1
Uid Success 1
Uid Failed 0
*****
GigabitEthernet0/0/2
*****
Profile Apply Success 1
Profile Apply Failed 0
Tunnel Config Apply Success 1
Tunnel Config Apply Fail 0
Tunnel Creation Failures 0
Connector Global Statistics:
=====
Total Number of Route Lookups: 0
Total Number of Whitelisted Packets: 0
Connector WAN Statistics:
=====
WAN interface :GigabitEthernet0/0/2
Total Number of Packets redirected: 0
Total Number of NSH encaps added to connector traffic: 0
Total Number of Pkts dropped because of fail-close:
```


How to Configure Cloud Web Security Tunneling

Importing a Certificate in a Trustpoint

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint <i>name</i> Example: Device(config)# crypto pki trustpoint cws-trustpoint	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	revocation-check none Example: Device(ca-trustpoint)# revocation-check none	Checks the revocation status of a certificate.
Step 5	enrollment terminal Example: Device(ca-trustpoint)# enrollment terminal	Specifies the enrollment parameters of the CA.
Step 6	exit Example: Device(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	crypto pki authenticate <i>name</i> Example: Device(config)# crypto pki authenticate cws-trustpoint	Retrieves the CA certificate and authenticates it.
Step 8	exit Example: Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Example

The following is a sample output of this task.

```
Device(config)# crypto pki trustpoint cws-trustpoint
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# exit
Device(config)# crypto pki authenticate cws-trustpoint

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

----BEGIN CERTIFICATE----
MIIGxDCCBKygAwIBAgIUdRcWd4PQQ361VsNXlG5FY7jr06wwDQYJKoZIhvcNAQEL
3aWQUVv/iyXULXT87EgL3b8zzf8fhTS7r654m9WM2W7pFqfimx9qAlFe9XcVlZrUu
.
.

EZAHFZ3Zivg2BaD4tOISO8/T2FDjG7PNUv0tgPAOKw2t94B+1evrSUhqJDU0Wf9c
9vkaKoPvX4w=
----END CERTIFICATE----
```

Trustpoint 'cws-trustpoint' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
 Fingerprint MD5: 1135E326 56E5AADF 53A4DD32 C8D5590F
 Fingerprint SHA1: AC4A728B 4DFC3560 1FA34B92 2422A42C 253F756C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Configuring Redirect and Whitelist

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	access-list <i>access-list-number</i> permit <i>source</i> <i>source-wildcard</i> Example: Device(config)# access-list 80 permit 10.10.20.0 0.0.0.255	Defines a standard IP access list which is referred when configuring the redirect list. The redirect list defines the client subnet behind the router interested in CWS.

	Command or Action	Purpose
Step 4	ip domain lookup Example: Device(config)# ip domain lookup	Enables IP Domain Name System (DNS)-based hostname-to-address resolution. This step and the following step is required to configure cloud bypass .
Step 5	ip name-server <i>server-address</i> Example: Device(config)# ip name-server 4.2.2.2	Specifies the address of one or more name servers to use for name and address resolution.
Step 6	crypto pki trustpool import url <i>url-name</i> Example: Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b	Installs the Cisco Trust-Store certificate from the specified URL. Whitelisting rules can be managed via CWS portal.
Step 7	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Parameter Map

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	parameter-map type cws-tunnel global Example: Device(config)# parameter-map type cws-tunnel global	Configures a global Cloud Web Security tunnel parameter-map and enters parameter-map type configuration mode.
Step 4	iwan	If you are setting up the Cloud Web Security, DMVPN and Spoke-to-Spoke tunnels from the same physical WAN interface of the Cisco 4000 Series ISR, IWAN must be configured under cws-tunnel global parameter-map. This will configure more specific match identity statements under cws ikev2 profile when the cws-tunnel out is configured on physical WAN interface.

	Command or Action	Purpose
Step 5	license {0 7} license Example: <pre>Device(config-profile)# license 7 AA4A545D7A53222E706D1A5D3B5D4E345E5B25737A737B6613724257425ABCA</pre>	Configures an encrypted license key that is sent to Cisco Cloud Web Security for authentication. <ul style="list-style-type: none"> • 7 configures a 66 characters hexadecimal encrypted license key. • 0 configures a 32 characters hexadecimal unencrypted license key.
Step 6	logging Example: <pre>Device(config-profile)# logging</pre>	Enables/disables the Cloud Web Security syslogs.
Step 7	primary Example: <pre>Device(config-profile)# primary</pre>	Configures a Cisco Cloud Web Security primary server for content scanning and enters CWS primary configuration mode.
Step 8	Do one of the following: <ul style="list-style-type: none"> • tower ipv4 ip-address • tower name server-name Example: <pre>Device(config-cws-pri)# tower ipv4 198.51.100.1</pre> Example: <pre>Device(config-cws-pri)# tower name access224.cws.sco.cisco.com</pre>	Configures the IPv4 address of the device or the name of the device on which the primary tunnel terminates. <p>Note The tower IP address or the tower name must be configured, not both. If you use the name, then you have to configure the Cisco 4000 series ISR for DNS resolution.</p>
Step 9	exit Example: <pre>Device(config-cws-pri)# exit</pre>	Exits CWS primary configuration mode and returns to parameter-map type configuration mode.
Step 10	secondary Example: <pre>Device(config-profile)# secondary</pre>	Configures a Cisco Cloud Web Security secondary server for content scanning and enters CWS secondary configuration mode.
Step 11	Do one of the following: <ul style="list-style-type: none"> • tower ipv4 ip-address • tower name server-name Example: <pre>Device(config-cws-sec)# tower ipv4 198.51.100.110</pre> Example: <pre>Device(config-cws-sec)# tower name access624.cws.sco.cisco.com</pre>	Configures the IPv4 address of the device or the name of the device on which the secondary tunnel terminates. <p>Note The tower IP address or the tower name must be configured, not both. If you use the name, then you have to configure the Cisco 4000 series ISR for DNS resolution.</p>
Step 12	exit Example: <pre>Device(config-cws-sec)# exit</pre>	Exits CWS secondary configuration mode and returns to parameter-map type configuration mode.

	Command or Action	Purpose
Step 13	fail-open Example: <pre>Device(config-profile)# fail-open</pre>	Configure passthrough for packets if Cloud Web Security towers are unavailable. The default mode is fail-close.
Step 14	redirect-list [<i>standard-acl</i>] Example: <pre>Device(config-profile)# redirect-list 80</pre>	Configures the redirect list, which is used to set the reverse route on the CWS Tower. Note This list does not indicate that packets will be redirected to this subnet only. By default, Cisco ISR 4000 Series Router redirects all web traffic to the CWS cloud, irrespective of whether the client subnets are configured under the redirect list or not. Under this scenario, clients that are not part of the redirect list are unable to get the return traffic back from the CWS Tower, for the clients which are not interested in CWS, those clients needs to be whitelisted to bypass the CWS Cloud.
Step 15	whitelist Example: <pre>Device(config-profile)# whitelist</pre>	Enables whitelisting of HTTP or secure HTTP traffic and prevents this traffic from entering Cloud Web Security towers.
Step 16	acl { <i>standard-acl</i> <i>extended-acl</i> name <i>named-acl</i> } Example: <pre>Device(config-cws-tun-wl)# acl name cws_whitelist Device(config-ext-nacl)#permit ip any 10.0.0.0 0.255.255.255 ==> Branch to HQ traffic Device(config-ext-nacl)#permit ip any 172.16.0.0 0.15.255.255 ==> Branch to HQ traffic Device(config-ext-nacl)#permit ip any 192.168.0.0 0.0.255.255 ==> Branch to HQ traffic</pre>	Specifies the access control list addresses of traffic that needs whitelisted. Standard, extended and named ACL are supported. Note It is recommend to whitelist RFP1918 addresses.
Step 17	domain-name regex <i>name</i> Example: <pre>Device(config-cws-tun-wl)# domain-name regex test</pre>	Specifies the name of regex parameter-map, which contains domain names to be whitelisted. Note The regex parameter map must be configured using the parameter-map type regex and pattern commands.
Step 18	download interval [<i>number</i>] Example: <pre>Device(config-cws-tun-wl)# download interval 5</pre>	(Optional) Specifies the interval in which white lists are downloaded from tower. <ul style="list-style-type: none"> The range is from 5 to 10080 minutes Note If this command is not specified it might indicate that there is whitelist to download from the tower.

	Command or Action	Purpose
Step 19	end Example: Device(config-profile)# end	Exits parameter-map type configuration mode and returns to privileged EXEC mode.

Enabling Cloud Web Security Tunnel Connector

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Configures an interface and enters interface configuration mode.
Step 4	cws-tunnel in Example: Device(config-if)# cws-tunnel in	Configures Cloud Web Security tunnel feature for ingress interface. <ul style="list-style-type: none"> • Configure the CWS parameter map with license, redirect list and primary tower before configuring cws-tunnel in • The inbound traffic on this interface is redirected for Cloud Web Security inspection, if the outbound interface for this traffic has the cws-tunnel out command configured on it. This is required to complete the CWS configuration.
Step 5	exit Example: Device(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 6	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 1/0/1	Configures an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 7	cws-tunnel out tunnel-number <i>tunnel-number</i> Example: Device(config-if)# cws-tunnel out tunnel-number 200	Configures the Cloud Web Security tunnel feature on the egress interface. <ul style="list-style-type: none"> • Configure the CWS parameter map with license, redirect list and primary tower before configuring cws-tunnel in • CWS creates 200 in primary and 201 in secondary tower. • Any HTTP or secure HTTP (HTTPS) traffic (that is not whitelisted) that is destined to this interface is subjected to Cloud Web Security redirection, if the ingress interface through which the traffic came through cws-tunnel in command configured on it. • The tunnel number can range from 0-65534.
Step 8	exit Example: Device(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

The **cws-tunnel out** command configuration creates the following entities:

- PKI trustpoint, *cws-trustpoint*
- Internet Key Exchange Protocol Version 2 (IKEv2) authorization policy, *cws-auth-policy*
- IKEv2 profile, *cws_ikev2_profile*
- IPsec profile, *cws_ipsec_profile*

What to do next

For step by step configuration, refer to *ISR - CWS Tunnel Based Redirection Step by Step Configuration* (<https://supportforums.cisco.com/document/12713171/isr-cws-tunnel-based-redirection-step-step-configuration>).

Verifying the Cloud Web Security Tunneling Configuration

Procedure

Step 1	enable Example: Device> enable Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	showcws-tunnel config Displays Cloud Web Security tunnel configuration information.

Example:

Device# **show cws-tunnel config**

```
cws-tunnel in configured on : GigabitEthernet0/0/0
cws-tunnel out configured on : GigabitEthernet0/0/2
Tunnel mapping (cws-tunnel out:Tunnel) is :
(GigabitEthernet0/0/2:Tunnel1000) (GigabitEthernet0/0/2:Tunnel1001)
cws-tunnel param-map config is :
Primary
  Tower IP                      : 10.147.106.139
Secondary
  Tower IP                      : 10.147.106.139
Whitelist Download interval    : 5
Whitelist acl(name/number)     : NONE
Domain-name regex              : NONE
License                        : XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Redirect-list                   : 1310
```

Step 3 **show cws-tunnel status**

Verifies if the Cloud Web Security tunnel is up or down.

Example:

Device# **show cws-tunnel status**

GigabitEthernet0/0/2-Tunnel1000: Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect

```
Interface: Tunnel1000
Profile: cws_ikev2_profile_1000
Uptime: 01:09:53
Session status: UP-ACTIVE
Peer: 10.147.106.139 port 4500 fvrf: (none) ivrf: (none)
  Phasel_id: 192.168.0.7
  Desc: (none)
  Session ID: 1
  IKEv2 SA: local 10.104.52.104/4500 remote 10.147.106.139/4500 Active
    Capabilities:DNX connid:1 lifetime:22:50:07
  IPSEC FLOW: permit 47 host 10.104.52.104 host 10.147.106.139
    Active SAs: 2, origin: crypto map
    Inbound:  #pkts dec'ed 160 drop 0 life (KB/Sec) 4607995/2868
    Outbound: #pkts enc'ed 263 drop 0 life (KB/Sec) 4607992/2868
```

```
*****
GigabitEthernet0/0/2-Tunnel1001:
*****
```

Step 4 **show cws-tunnel statistics**

Verifies if traffic is routed through the Cloud Web Security tunnel or not.

Example:

Device# **show cws-tunnel statistics**

```
Whitelist Download Success      0
Whitelist Download Failed      0
Uid Requests                    0
```

```

Uid Responses                                0
Uid Success                                0
Uid Failed                                  0
*****
GigabitEthernet0/0/2
*****
Profile Apply Success                        1
Profile Apply Failed                        0
Tunnel Config Apply Success                1
Tunnel Config Apply Fail                   0
Tunnel Creation Failures                   0

Connector Global Statistics:
=====

Total Number of Route Lookups:              0
Total Number of Whitelisted Packets:        0

Connector WAN Statistics:
=====

WAN interface :GigabitEthernet0/0/2
    Total Number of Packets redirected:      0
    Total Number of NSH encaps added to connector traffic: 0
    Total Number of Pkts dropped because of fail-close: 0
    Total Number of Pkts skipped because of fail-open: 0

```

Step 5 **show cws-tunnel whitelist**

Displays the Cloud Web Security tunnel whitelist configuration.

Example:

```

Device# show cws-tunnel whitelist

ACL configured via CLI :

ACL downloaded from tower :
Last modified time at tower : Wed, 02 Sep 2015 10:15:16 UTC

Domains configured via CLI
Domain-name regex: NONE

Domains downloaded from tower:
    www.google.com
    www.gap.com

```

Step 6 **show cws-tunnel whitelist stats**

Displays whitelist statistics information.

Example:

```

Device# show cws-tunnel whitelist stats

Total  Last dwld
WL download request:      14      1
SSL failures:             0        0
WL download response:     14      1
    success response:      3        0
    no config change:     11      1

```

```

no config: 0 0
other responses(Other than 200/304/404): 0 0
other failures(no encoding/HTTP version): 0 0
XML parse errors: 0 0
Memory failures: 0 0

XML parser stats:
  Src ACEs Dst ACEs
    0 0
Last download request time: 2015-09-02T10:45:53+0000

```

Step 7 **show ipdns-snoop all**

Displays all DNS snoop entries.

Example:

```
Device# show ip dns-snoop all
```

IP Address	Client(s)	Expire	Match
202.3.77.184	1	3513	www.example.com

Step 8 **show platform hardware qfp active feature cws datapath config**

Displays Cloud Web Security configuration information in the Cisco Quantum Flow Processor (QFP).

Example:

```
Device# show platform hardware qfp active feature cws datapath config
```

```

Data Path Configs:
Mode           : Connector
Fail-open config: OFF
Inflow Debugging:
WL Policy-ID    : 536870912

CWS IN
=====
GigabitEthernet0/0/0

CWS OUT
=====
GigabitEthernet0/0/2
  -Tunnel1000 (primary adj : f80000e6)
  -Tunnel1001 (secondary adj: 0)

```

Step 9 **show platform hardware qfp active feature dns-snoop-agent client pattern-list**

Example:

```
Device# show platform hardware qfp active feature dns-snoop-agent client pattern-list
```

```

Pattern List in CPP client: 3

Name: cisco.com
feature_mask: 0x00000001, hw_ptr: 0xe8d3d000

Name: ibm.com
feature_mask: 0x00000001, hw_ptr: 0xe8d3d220

```

```
Name: www.iitk.ac.in
feature_mask: 0x00000001, hw_ptr: 0xe8d3d110
```

Step 10 **show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list**

Example:

```
Device# show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list
```

```
Name: cisco.com
feature_mask: 1, dirty: 0, ref_count: 0, Match count: 0
```

```
Name: ibm.com
feature_mask: 1, dirty: 0, ref_count: 0, Match count: 0
```

```
Name: www.iitk.ac.in
feature_mask: 1, dirty: 0, ref_count: 1, Match count: 0
```

Step 11 **show platform hardware qfp active feature cws datapath stats**

Displays Cloud Web Security configuration information in the Cisco Quantum Flow Processor (QFP).

Example:

```
Device# show platform hardware qfp active feature cws datapath stats
```

```
Connector Global Statistics:
=====
```

```
Total Number of Route Lookups:                0
Total Number of Whitelisted Packets:            0
```

```
Connector WAN Statistics:
=====
```

```
WAN interface :GigabitEthernet0/0/2
  Total Number of Packets redirected:            0
  Total Number of NSH encaps added to connector traffic: 0
  Total Number of Pkts dropped because of fail-close: 0
  Total Number of Pkts skipped because of fail-open: 0
```

Step 12 **show platform hardware qfp active feature dns-snoop-agent datapath stats**

Displays Cloud Web Security configuration information in the Cisco Quantum Flow Processor (QFP).

Example:

```
Device# show platform hardware qfp active feature dns-snoop-agent datapath stats
```

```
DNS Snoop Agent Stats:
  parser unknown pkt: 180
  parser fmt error: 0
  parser pa error: 0
  parser non resp: 0
  parser multiple name: 0
  parser dns name err: 0
  parser matched ip: 1
  parser skip: 0
  regex locked: 0
  regex not matched: 32
  entries in use: 1
  ip cache allocation fail: 0
  ip addr add: 1
  ip addr update: 0
```

```

ip addr delete: 0
ip addr cache hit: 1
ip addr cache miss: 77
ip addr bad param: 0
ip addr delete not found: 0
ip cache not initialized: 0

```

Step 13 show platform hardware qfp active classification class-group-manager class-group client cws 2100

Example:

Device# **show platform hardware qfp active classification class-group-manager class-group client cws 2100**

```

class-group client cws 2100
class-group [cws-cg:2100] (classes: 1)
clients:
fields: ipv4_src:3 ipv4_dst:3 (c000:0:0:00000000)
(1) class: match-any [2100.1] (filters: 1)
    (1) filter: generic [2100.1.1] (rules: 3)
        (10) rule: generic [2100.1.1.2] (permit)
            match ipv4_src 1.1.1.0 0.0.0.255
            match ipv4_dst any
        (20) rule: generic [2100.1.1.3] (permit)
            match ipv4_src 2.2.2.0 0.0.0.255
            match ipv4_dst any
        (30) rule: generic [2100.1.1.4] (permit)
            match ipv4_src 3.3.3.0 0.0.0.255
            match ipv4_dst any

```

Additional References for Cloud Web Security Tunneling

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	<ul style="list-style-type: none"> • Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
Cisco ScanCenter Administrator Guide	Cisco ScanCenter Administrator Guide, Release 5.2
Zone-based firewall configuration	Zone-Based Policy Firewalls
CWS Tunnel Based Redirection Configuration	<i>ISR - CWS Tunnel Based Redirection Step by Step Configuration</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cloud Web Security Tunneling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Cloud Web Security Tunneling

Feature Name	Releases	Feature Information
Cloud Web Security Tunneling	Cisco IOS XE Release 3.16S	<p>Cisco Cloud Web Security is a cloud-delivered web security solution. Cloud Web Security offers extensive security as a service.</p> <p>Cloud Web Security controls access to websites and specific content in web pages and applications. Administrators can set and enforce specific web use policies across the network for applications, websites and specific webpage content.</p> <p>In Cisco ISR 4400 Series Integrated Services Routers, Cloud Web Security is delivered through a tunneling method. HTTP and HTTPS traffic from ISR 4400 Series Router to Cloud Web Security is transported through IPsec over generic routing encapsulation (GRE) tunnels. CSR 1000V Series Cloud Services Routers are configured at the tunnel endpoints and are connected to Cloud Tunnel Relay (CTR). CTR resides in data centers that host Cloud Web Security towers.</p> <p>The following command was introduced or modified: parameter-map type cws-tunnel global, license, logging, primary, tower ipv4, tower name, secondary, fail-open, redirect-list, whitelist, interface, cws-tunnel in, cws-tunnel out.</p>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.