VRF-Aware Cloud Web Security

The VRF-Aware Cloud Web Security feature adds virtual routing and forwarding (VRF) support to the Cisco Cloud Web Security configuration. VRF instances in IP-based networks enable a device to have multiple instances of the routing table at the same time. Because routing instances are independent of each other, they can use the same IP addresses without any conflict.

This feature describes the VRF-Aware Cloud Web Security feature and explains how to configure it.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Restrictions for VRF-Aware Cloud Web Security

- While enabling a virtual routing and forwarding (VRF) instance on a device, configure the **content-scan out** command only on one interface to ensure that the tower polling mechanism is consistent.
- The VRF-Aware Cloud Web Security feature works only in VRF-Lite scenarios.

- Overlapping IP addresses must be resolved if multiple VRF instances converge into a single VRF.

Information About VRF-Aware Cloud Web Security

VRF-Aware Cloud Web Security Overview

Cisco Cloud Web Security provides content scanning of HTTP and secure HTTP (HTTPS) traffic and malware protection services to web traffic. It also helps devices transparently redirect HTTP and HTTPS traffic to the Cisco Web Security cloud. The VRF-Aware Cloud Web Security feature adds virtual routing and forwarding (VRF) support to Cisco Cloud Web Security.

VRF instances in IP-based networks enable a device to have multiple instances of the routing table at the same time. Because routing instances are independent of each other, they use the same IP addresses without any conflict.

You can use VRFs with or without Multiprotocol Label Switching (MPLS). When VRFs are used without MPLS, it is called VRF-Lite. The VRF-Aware Cloud Web Security feature works only in VRF-Lite scenarios.

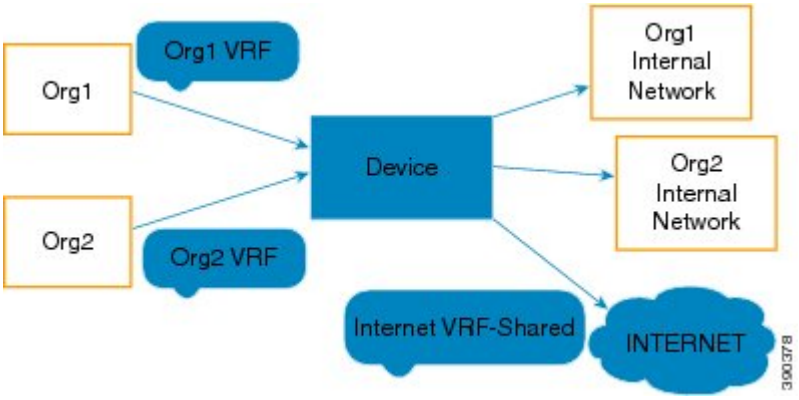
During content scan, the egress VRF ID of the interface on which the **content-scan out** command is configured is used. The VRF ID that is used during communication with the Cloud Web Security tower is same as the VRF ID of the interface on which the **content-scan out** command is configured. Based on your configuration, include the routes configured in the Cloud Web Security tower in the appropriate VRFs.

The whitelisted traffic flows through the interface on which the VRF that is connected to the Internet is configured. A whitelist is an approved list of entities that are provided a particular privilege, service, mobility, access, or recognition. Whitelisting means to grant access.

VRF-Aware Cloud Web Security Scenarios

This section describes some scenarios in which the VRF-Aware Cloud Web Security is configured:

Figure 1: VRF-Aware Cloud Web Security: Scenario 1

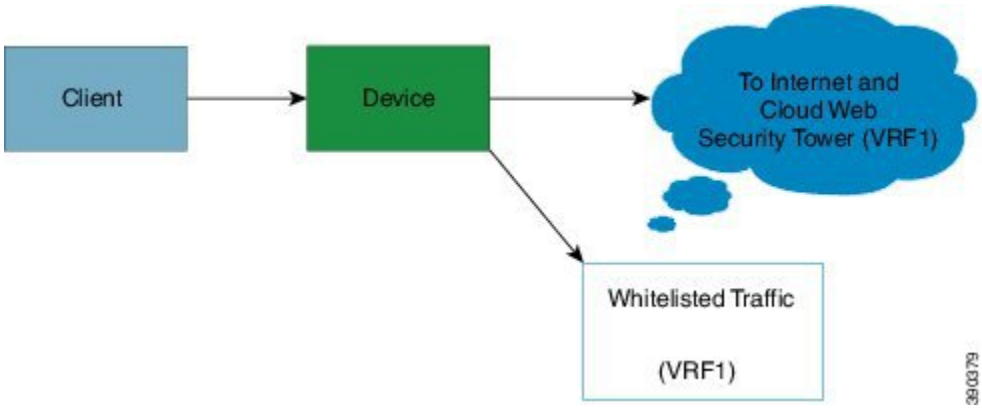


In the illustration above, there are two separate networks, Org1 and Org2. The device provides connectivity to the Internet as a shared service between these organizations. Because each organization has a separate

virtual routing and forwarding (VRF) instance, both have their individual routing table entries. The clients on Org1 and Org2 can both have the same IP addresses and still access the internal network of their organization.

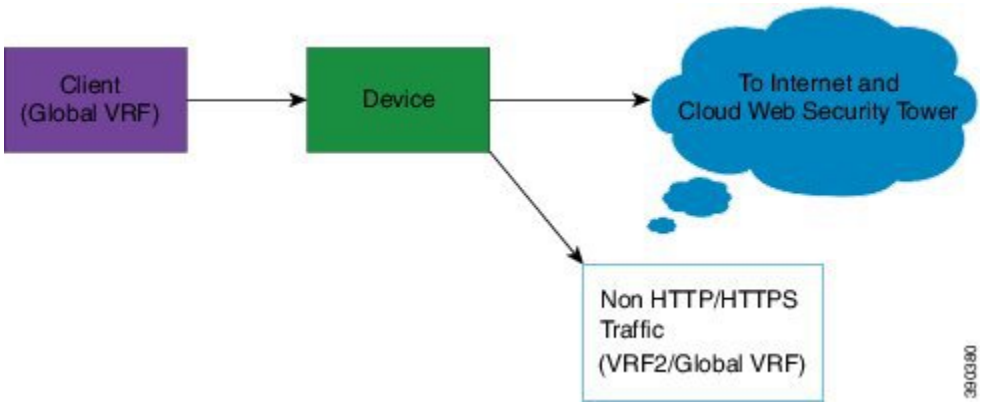
Because the Internet VRF is shared, Network Address Translation (NAT) must be configured to distinguish the traffic from both the networks. Also, the respective routes from Org1 and Org2 must be advertised into the Internet VRF and vice versa, for proper routing of traffic. In Scenario 1, you can enable Cisco Cloud Web Security on the VRF-shared Internet. Enabling Cisco Cloud Web Security ensures that the HTTP and secure HTTP (HTTPS) traffic is redirected to the configured Cloud Web Security tower. Traffic is passed to the internal networks of both organizations through whitelisting.

Figure 2: VRF-Aware Cloud Web Security: Scenario 2



In the illustration above, clients belong to a global VRF. The Internet traffic belongs to another VRF, VRF1. Whitelisted traffic also uses VRF1 because the interface that is configured for content scan must be connected to whitelisted sites. When you configure content scan on interfaces, each interface will have a unique VRF.

Figure 3: VRF-Aware Cloud Web Security: Scenario 3



In the illustration above, the client traffic comes into the global VRF. All HTTP and HTTPS traffic is sent to VRF1, and non-HTTP and non-HTTPS traffic is sent to VRF2/global VRF. Content scan redirects the HTTP/HTTPS traffic to the Cloud Web Security tower. The classification of HTTP/HTTPS traffic must be done before content-scan redirection.

How to Configure VRF-Aware Cloud Web Security

In Cisco IOS Release 15.4(2)T, some of the Cloud Web Security commands were replaced by new commands. Releases prior to Cisco IOS Release 15.4(2)T still use the old commands.

This section consists of tasks that use the commands existing prior to Cisco IOS Release 15.4(2)T and a corresponding task that uses the commands introduced or modified in the Cisco IOS Release 15.4(2)T.

Configuring a Cloud Web Security Tower in Cisco IOS Release 15.4(2)T and Later Releases

Note This task applies to Cisco IOS Release 15.4(2)T and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type cws global**
4. **server primary ipv4** *ipv4-address* **port http** *port-number* **https** *port-number*
5. **server secondary name** *name* **port http** *port-number* **https** *port-number*
6. **license** {**0** | **7**} *authentication-key*
7. **source address ipv4** *ipv4-address*
8. **timeout server** *seconds*
9. **timeout session-inactivity** *seconds*
10. **user-group** *name* [**username** *name*]
11. **server on-failure** {**allow-all** | **block-all**}
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**parameter-map type cws global** **Example:** `Device(config)# parameter-map type cws global`	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.
Step 4	**server primary ipv4** *ipv4-address* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server primary ipv4 10.2.2.2 port http 8080 https 8080`	Configures a Cisco Cloud Web Security primary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 5	**server secondary name** *name* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server secondary name example1363.example.net port http 8080 https 8080`	Configures a Cisco Cloud Web Security secondary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 6	**license** {**0** | **7**} *authentication-key* **Example:** `Device(config-profile)# license 0 F52409C9DAF22005CF33E64A7BC524C9`	Configures an unencrypted license key that is sent to Cisco Cloud Web Security for authentication. • To configure an encrypted license key, use the **7** keyword and specify an authentication key of 66 hexadecimal characters.
Step 7	**source address ipv4** *ipv4-address* **Example:** `Device(config-profile)# source address ipv4 192.168.4.4`	Configures the source address for content scan redirection.
Step 8	**timeout server** *seconds* **Example:** `Device(config-profile)# timeout server 20`	Specifies a server keepalive time in seconds.
Step 9	**timeout session-inactivity** *seconds* **Example:** `Device(config-profile)# timeout session-inactivity 180`	Specifies the session inactivity time in seconds.
Step 10	**user-group** *name* [**username** *name*] **Example:** `Device(config-profile)# user-group group1 username user1`	Specifies a default user group.

	Command or Action	Purpose
Step 11	**server on-failure** {**allow-all** | **block-all**} **Example:** `Device(config-profile)# server on-failure block-all`	Blocks all traffic to a web server when communication between the web server and the Cisco Cloud Web Security server fails.
Step 12	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Configuring a Cloud Web Security Tower

Note This task applies to releases prior to Cisco IOS Release 15.4(2)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type content-scan global**
4. **server scansafe primary ipv4** *ipv4-address* **port http** *port-number* **https** *port-number*
5. **server scansafe secondary name** *name* **port http** *port-number* **https** *port-number*
6. **license** {**0** | **7**} *authentication-key*
7. **source address ipv4** *ipv4-address*
8. **timeout server** *seconds*
9. **timeout session-inactivity** *seconds*
10. **user-group** *name* [**username** *name*]
11. **server scansafe on-failure** {**allow-all** | **block-all**}
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type content-scan global** **Example:** `Device(config)# parameter-map type content-scan global`	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.
Step 4	**server scansafe primary ipv4** *ipv4-address* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server scansafe primary ipv4 10.2.2.2 port http 8080 https 8080`	Configures a Cisco Cloud Web Security primary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 5	**server scansafe secondary name** *name* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server scansafe secondary name example1363.example.net port http 8080 https 8080`	Configures a Cisco Cloud Web Security secondary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 6	**license** {**0** | **7**} *authentication-key* **Example:** `Device(config-profile)# license 0 F52409C9DAF22005CF33E64A7BC524C9`	Configures an unencrypted license key that is sent to Cisco Cloud Web Security for authentication. • To configure an encrypted license key, use the **7** keyword and specify an authentication key of 66 hexadecimal characters.
Step 7	**source address ipv4** *ipv4-address* **Example:** `Device(config-profile)# source address ipv4 192.168.4.4`	Configures the source address for content scan redirection.
Step 8	**timeout server** *seconds* **Example:** `Device(config-profile)# timeout server 20`	Specifies a server keepalive time in seconds.
Step 9	**timeout session-inactivity** *seconds* **Example:** `Device(config-profile)# timeout session-inactivity 180`	Specifies the session inactivity time in seconds.

	Command or Action	Purpose
Step 10	**user-group** *name* [**username** *name*] **Example:** `Device(config-profile)# user-group group1 username user1`	Specifies a default user group.
Step 11	**server scansafe on-failure** {**allow-all** | **block-all**} **Example:** `Device(config-profile)# server scansafe on-failure block-all`	Blocks all traffic to a web server when communication between the web server and the Cisco Cloud Web Security server fails.
Step 12	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Configuring VRF-Aware Cloud Web Security in Cisco IOS Release 15.4(2)T and Later Releases

Note This task applies to Cisco IOS Release 15.4(2)T and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **exit**
5. **interface** *type number*
6. **ip vrf forwarding** *name*
7. **ip address** *ip-address mask*
8. **cws out**
9. **ip virtual-reassembly in**
10. **ip virtual-reassembly out**
11. **duplex auto**
12. **speed auto**
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Device(config)# ip vrf output`	Defines a virtual routing and forwarding (VRF) instance and enters VRF configuration mode.
Step 4	**exit** **Example:** `Device(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 5	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0`	Configures an interface and enters interface configuration mode.
Step 6	**ip vrf forwarding** *name* **Example:** `Device(config-if)# ip vrf forwarding output`	Associates a VRF instance and configures a VRF forwarding table on an interface.
Step 7	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.4.4 255.255.255.0`	Configures an IP address for an interface.
Step 8	**cws out** **Example:** `Device(config-if)# cws out`	Configures the egress interface for Cloud Web Security content scanning.
Step 9	**ip virtual-reassembly in** **Example:** `Device(config-if)# ip virtual-reassembly in`	Enables Virtual Fragment Reassembly (VFR) on the ingress.
Step 10	**ip virtual-reassembly out** **Example:** `Device(config-if)# ip virtual-reassembly out`	Enables VRF on the egress.

	Command or Action	Purpose
Step 11	**duplex auto** **Example:** `Device(config-if)# duplex auto`	Enables autonegotiation on an interface.
Step 12	**speed auto** **Example:** `Device(config-if)# speed auto`	Configures the speed of an interface.
Step 13	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

Configuring VRF-Aware Cloud Web Security

Note This task applies to releases prior to Cisco IOS Release 15.4(2)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **exit**
5. **interface** *type number*
6. **ip vrf forwarding** *name*
7. **ip address** *ip-address mask*
8. **content-scan out**
9. **ip virtual-reassembly in**
10. **ip virtual-reassembly out**
11. **duplex auto**
12. **speed auto**
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Device(config)# ip vrf output`	Defines a virtual routing and forwarding (VRF) instance and enters VRF configuration mode.
Step 4	**exit** **Example:** `Device(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 5	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0`	Configures an interface and enters interface configuration mode.
Step 6	**ip vrf forwarding** *name* **Example:** `Device(config-if)# ip vrf forwarding output`	Associates a VRF instance and configures a VRF forwarding table on an interface.
Step 7	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.4.4 255.255.255.0`	Configures an IP address for an interface.
Step 8	**content-scan out** **Example:** `Device(config-if)# content-scan out`	Configures the egress interface for content scanning.
Step 9	**ip virtual-reassembly in** **Example:** `Device(config-if)# ip virtual-reassembly in`	Enables Virtual Fragment Reassembly (VFR) on the ingress.
Step 10	**ip virtual-reassembly out** **Example:** `Device(config-if)# ip virtual-reassembly out`	Enables VRF on the egress.

	Command or Action	Purpose
Step 11	**duplex auto** **Example:** `Device(config-if)# duplex auto`	Enables autonegotiation on an interface.
Step 12	**speed auto** **Example:** `Device(config-if)# speed auto`	Configures the speed of an interface.
Step 13	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

Configuration Examples for VRF-Aware Cloud Web Security

Example: Configuring a Cloud Web Security Tower in Cisco IOS Release 15.4(2)T and Later Releases

Note This example applies to Cisco IOS Release 15.4(2)T and later releases.

```
Device# configure terminal
Device(config)# parameter-map type cws global
Device(config-profile)# server primary ipv4 10.2.2.2 port http 8080 https 8080
Device(config-profile)# server secondary name example1363.example.net port http 8080 https
 8080
Device(config-profile)# license 0 F52409C9DAF22005CF33E64A7BC524C9
Device(config-profile)# source address ipv4 192.168.4.4
Device(config-profile)# timeout server 20
Device(config-profile)# timeout session-inactivity 180
Device(config-profile)# user-group group1 username user1
Device(config-profile)# server on-failure block-all
Device(config-profile)# end
```

Example: Configuring a Cloud Web Security Tower

Note This example applies to releases prior to Cisco IOS Release 15.4(2)T.

```
Device# configure terminal
Device(config)# parameter-map type content-scan global
Device(config-profile)# server scansafe primary ipv4 10.2.2.2 port http 8080 https 8080
Device(config-profile)# server scansafe secondary name example1363.example.net port http
```

```
8080 https 8080
Device(config-profile)# license 0 F52409C9DAF22005CF33E64A7BC524C9
Device(config-profile)# source address ipv4 192.168.4.4
Device(config-profile)# timeout server 20
Device(config-profile)# timeout session-inactivity 180
Device(config-profile)# user-group group1 username user1
Device(config-profile)# server scansafe on-failure block-all
Device(config-profile)# end
```

Example: VRF-Aware Cloud Web Security in Cisco IOS Release 15.4(2)T and Later Releases

Note This example applies to Cisco IOS Release 15.4(2)T and later releases.

```
Device# configure terminal
Device(config)# ip vrf output
Device(config-vrf)# exit
Device(config)# interface gigabitethernet 0/0
Device(config-if)# ip vrf forwarding output
Device(config-if)# ip address 192.168.4.4 255.255.255.0
Device(config-if)# cws out
Device(config-if)# ip virtual-reassembly in
Device(config-if)# ip virtual-reassembly out
Device(config-if)# duplex auto
Device(config-if)# speed auto
Device(config-if)# end
```

Example: Configuring VRF-Aware Cloud Web Security

Note This example applies to releases prior to Cisco IOS Release 15.4(2)T.

```
Device# configure terminal
Device(config)# ip vrf output
Device(config-vrf)# exit
Device(config)# interface gigabitethernet 0/0
Device(config-if)# ip vrf forwarding output
Device(config-if)# ip address 192.168.4.4 255.255.255.0
Device(config-if)# content-scan out
Device(config-if)# ip virtual-reassembly in
Device(config-if)# ip virtual-reassembly out
Device(config-if)# duplex auto
Device(config-if)# speed auto
Device(config-if)# end
```

Additional References for VRF-Aware Cloud Web Security

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Firewall commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for VRF-Aware Cloud Web Security

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 1: Feature Information for VRF-Aware Cloud Web Security

Feature Name	Releases	Feature Information
VRF-Aware Cloud Web Security	15.4(1)T 15.4(2)T	The VRF-Aware Cloud Web Security feature adds virtual routing and forwarding (VRF) support to the Cisco Cloud Web Security configuration. VRF instances in IP-based networks enable a device to have multiple instances of the routing table at the same time. Because routing instances are independent of each other, they can use the same IP addresses without any conflict. The following command was introduced or modified: **show content-scan**. In Cisco IOS Release 15.4(2)T, the **show content-scan** command was replaced by the **show cws** command.