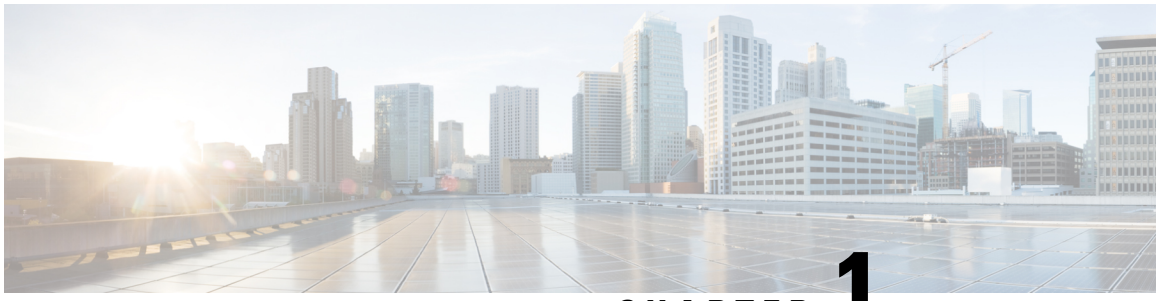
Security Configuration Guide: Cisco Umbrella Integration, Cisco IOS XE Gibraltar 16.11.x

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

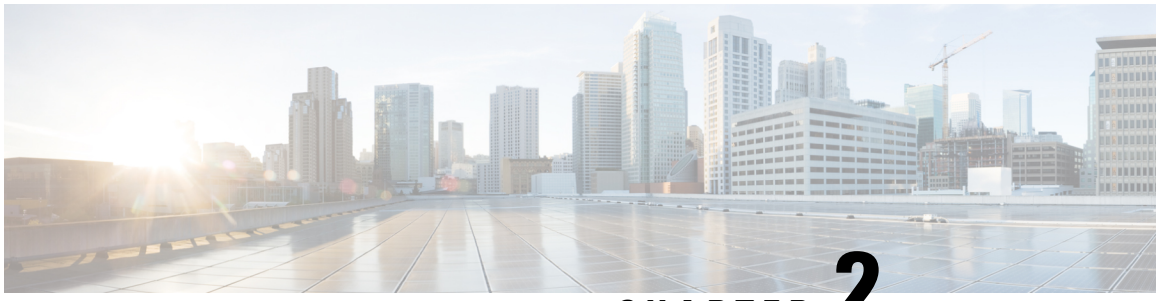
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.



CHAPTER 2

Cisco Umbrella Integration

The Cisco Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device. The security administrator configures policies on the Cisco Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). Cisco device acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Cisco Umbrella portal. This feature is available on Cisco IOS XE Denali 16.3 and later releases.

Restrictions for Cisco Umbrella Integration

- If an application or host uses IP address directly instead of DNS to query domain names, policy enforcement is not applied.
- When the client is connected to a web proxy, the DNS query does not pass through the Cisco device. In this case, the connector does not detect any DNS request and the connection to the web server bypasses any policy from the Cisco Umbrella portal.

- When the Cisco Umbrella Integration policy blocks a DNS query, the client is redirected to a Cisco Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Cisco Umbrella portal.
- User authentication and identity is not supported in this release.
- The type A, AAAA, and TXT queries are the only records that are redirected. Other types of query bypasses the connector. Cisco Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Cisco Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to Cisco Umbrella cloud for further inspection.
- Only the IPv4 address of the host is conveyed in the EDNS option.
- A maximum of 64 local domains can be configured, and the allowed domain name length is 100 characters.

Prerequisites for Cisco Umbrella Integration

Before you configure the Cisco Umbrella Integration feature, ensure that the following are met:

- The device has a security K9 license to enable Cisco Umbrella Integration.
- The device runs the Cisco IOS XE Denali 16.3 software image or later.
- Cisco Umbrella subscription license is available.
- The device is set as the default DNS server gateway and needs to ensure that the DNS traffic goes through the Cisco device.
- Communication for device registration to the Cisco Umbrella server is via HTTPS. This requires a root certificate to be installed on the router. To download this certificate directly from a link instead of pasting it in, you can find the certificate here: https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt.

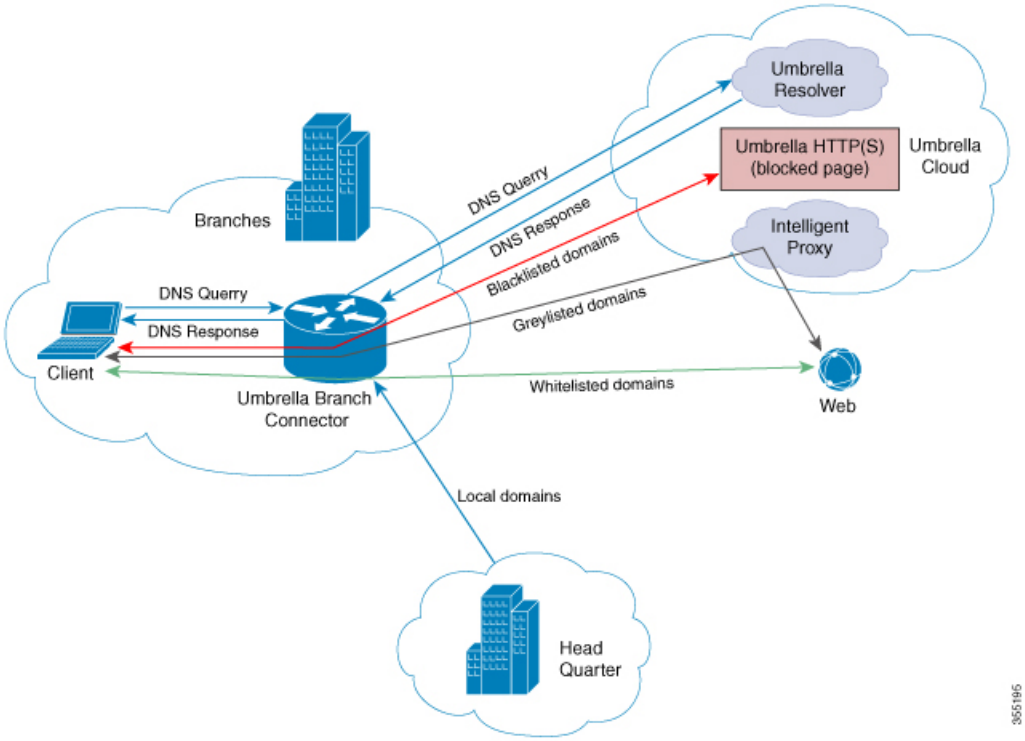
Cloud-based Security Service Using Cisco Umbrella Integration

The Cisco Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through the device. When a host initiates the traffic and sends a DNS query, the Cisco Umbrella Connector in the device intercepts and inspects the DNS query. If the DNS query is for a local domain, it forwards the query without changing the DNS packet to the DNS server in the enterprise network. If it is for an external domain, it adds an Extended DNS (EDNS) record to the query and sends it to Cisco Umbrella Resolver. An EDNS record includes the device identifier information, organization ID and client IP. Based on this information, Cisco Umbrella Cloud applies different policies to the DNS query.

The Umbrella Integration cloud, based on the policies configured on the portal and the reputation of the DNS Fully Qualified Domain Name (FQDN) may take one of the following actions:

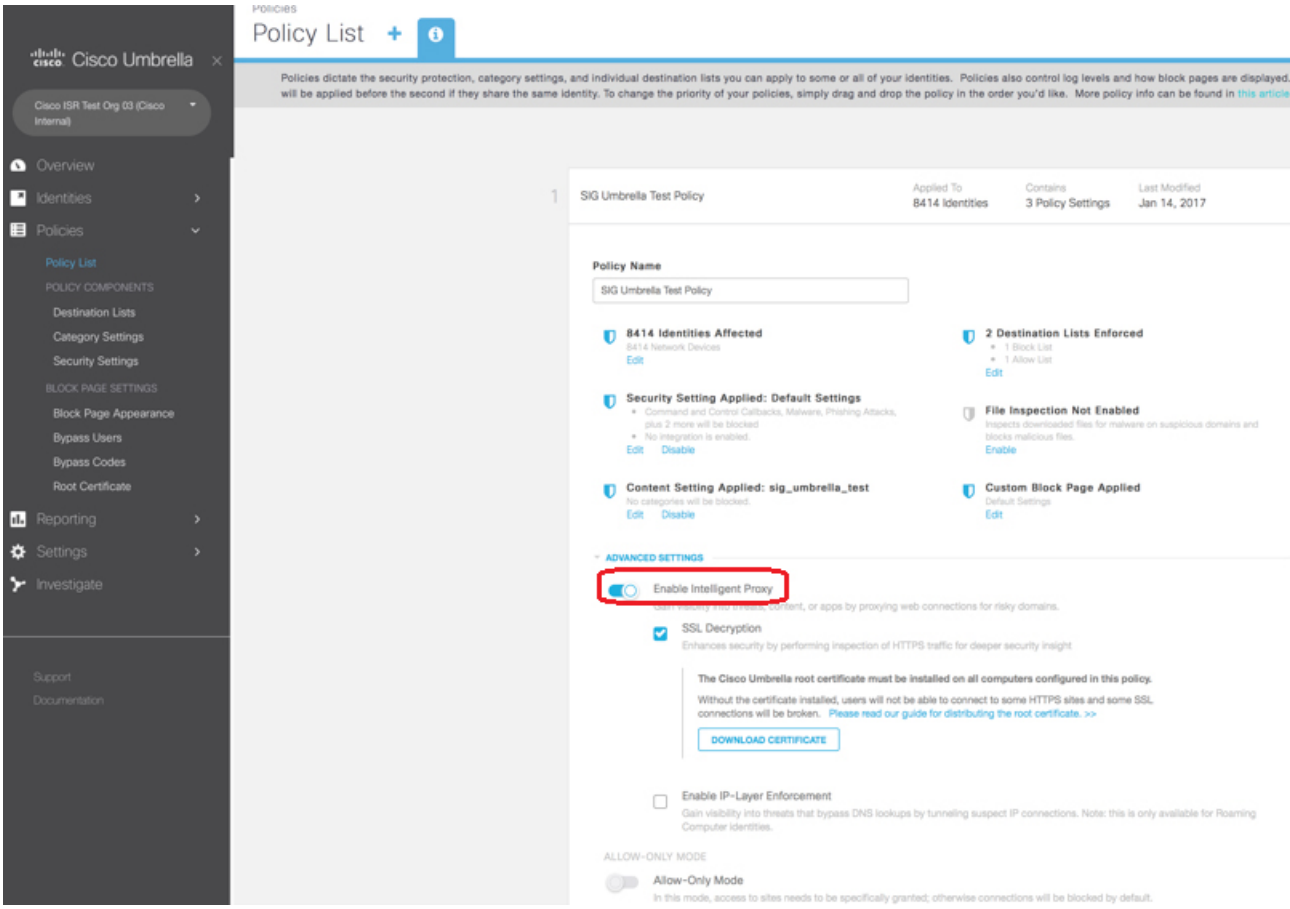
- If FQDN is found to be malicious or blocked by the customized Enterprise Security policy, then the IP address of the Umbrella Cloud's blocked landing page is returned in the DNS response. This is called a blacked list action at Umbrella Cloud.
- If FQDN is found to be non-malicious, then the IP address of the content provider is returned in the DNS response. This is called a whitelist action at Umbrella Cloud.

- If the FQDN is suspicious, then the intelligent proxy unicast IP addresses are returned in the DNS response. This is referred to as grey list action at Umbrella cloud.



When the DNS response is received, the device forwards the response back to the host. The host will extract the IP address from the response and send the HTTP / HTTPS requests to this IP.

Note The intelligent proxy option has to be enabled in the Umbrella dashboard for the Umbrella Resolver to return the intelligent proxy unicast IP addresses in the DNS response when an attempt is made to access the domains in the grey list.



Handling HTTP and HTTPs Traffic

With Cisco Umbrella Integration, HTTP and HTTPs client requests are handled in the following ways:

- If the Fully Qualified Domain Name (FQDN) in the DNS query is malicious (falls under blacklisted domains), Umbrella Cloud returns the IP address of the blocked landing page in the DNS response. When the HTTP client sends a request to this IP, Umbrella Cloud displays a page that informs the user that the requested page was blocked and the reason for blocking the page.

  If the FQDN in the DNS query is non-malicious (falls under whitelisted domains), Umbrella Cloud returns the IP address of the content provider. The HTTP client sends the request to this IP address and gets the desired content.

  If the FQDN in the DNS query falls under grey-listed domains, Umbrella Resolver returns the unicast IP addresses of intelligent proxy in the DNS response. All HTTP traffic from the host to the grey domain gets proxied through the intelligent proxy and undergo URL filtering.

One potential limitation in using intelligent proxy unicast IP addresses is the probability of the datacenter going down when the client is trying to send the traffic to the intelligent proxy unicast IP address. This is a scenario where a client has completed DNS resolution for a domain which falls under grey-listed domain and client's HTTP/(S) traffic is being sent to one of the obtained intelligent proxy unicast IP address. If that datacenter is down, then the client has no way of knowing it.

The Umbrella Connector does not act on the HTTP and HTTPS traffic. The connector does not redirect any web traffic or alter any HTTP/(S) packets.

Encrypting the DNS Packet

The DNS packet sent from the Cisco device to Cisco Umbrella Integration server must be encrypted if the EDNS information in the packet contains information such as user IDs, internal network IP addresses, and so on. When the DNS response is sent back from the DNS server, device decrypts the packet and forwards it to the host.

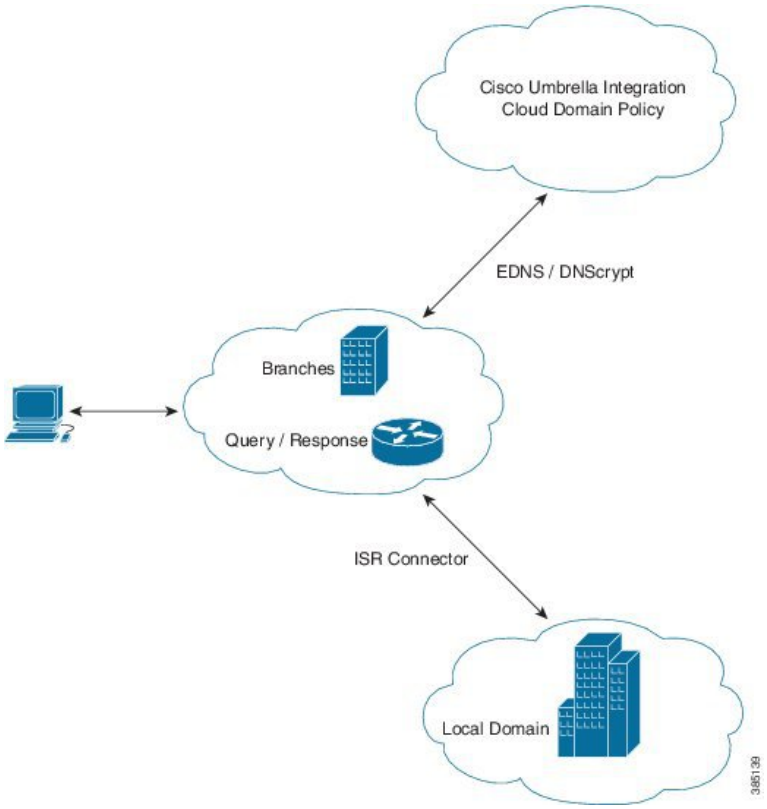
You can encrypt DNS packets only when the DNScrypt feature is enabled on the Cisco device.

The Cisco device uses the following Anycast recursive Cisco Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

The Figure 1 describes the Cisco Umbrella Integration topology.

Figure 1: Cisco Umbrella Integration Topology



Benefits of Cisco Umbrella Integration

Cisco Umbrella Integration provides security and policy enforcement at DNS level. It enables the administrator to split the DNS traffic and directly send some of the desired DNS traffic to a specific DNS server (DNS server located within the enterprise network). This helps the administrator to bypass the Cisco Umbrella Integration.

Configure the Cisco Umbrella Connector

To configure Cisco Umbrella Connector:

- Get the API token from the Cisco Umbrella registration server.
- Have the root certificate establish the HTTPS connection with the Cisco Umbrella registration server. Import the root certificate of DigiCert given below into the device using the **crypto pki trustpool import terminal** command.

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

- Verify that the PEM import is successful. A message is displayed after importing the certificate.

This is the sample configuration:

```
enable
configure terminal
parameter-map type umbrella global
 token AABBA59A0BDE1485C912AFE472952641001EEECC

exit
```

Registering the Cisco Umbrella Tag

To register the Cisco Umbrella tag, perform these steps:

1. Configure the umbrella parameter map as shown in the previous section.
2. Configure **umbrella out** on the WAN interface:

```
interface gigabitEthernet 0/0/1
 umbrella out
```

3. Configure **umbrella in** on the LAN interface:

```
interface gigabitEthernet 0/0/0.4
 umbrella in mydevice_tag
```

Note For the Cisco devices, the length of the hostname and umbrella tag should not exceed 49 characters.

4. After you configure **umbrella in** with a tag using the **umbrella in mydevice_tag** command, the device registers the tag to the Cisco Umbrella Integration portal.
5. The device initiates the registration process by resolving *api.opendns.com*. You need to have a name server (*ip name-server x.x.x.x*) and domain lookup (*ip domain-lookup*) configured on the device to successfully resolve the FQDN.

Note You should configure the **umbrella out** command before you configure **umbrella in** command. Registration is successful only when the port 443 is in *open* state and allows the traffic to pass through the existing firewall.

Configuring Cisco Device as a Pass-through Server

You can identify the traffic to be bypassed using domain names. In the Cisco device, you can define these domains in the form of regular expressions. If the DNS query that is intercepted by the device matches one of the configured regular expressions, then the query is bypassed to the specified DNS server without redirecting to the Cisco Umbrella cloud. This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

```
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.fisco.com
Device(config)# pattern .*engineering.fisco.*

Attach the regex param-map with the openDNS global configuration as shown below:

Device(config)# parameter-map type umbrella global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
Device(config-profile)# local-domain dns_bypass
```

DNSCrypt, Resolver, and Public-key

When you configure the device using the **parameter-map type umbrella global** command, the following values are auto-populated:

- DNSCrypt
- Resover IP
- Public-Key

We recommend that you change the above parameters only when you perform certain tests in the lab. These parameters are reserved for future use. If you modify these parameters, it can affect the normal functioning of the device.

Resolver

The following commands change the redirection of DNS packets from the Cisco device to Cisco Umbrella cloud:

- **resolver ipv4** *1.1.1.1*
- **resolver ipv4** *1.1.1.2*
- **resolver ipv6** *1234::1*
- **resolver ipv6** *2345::1*

In this example, all the IPv4 DNS packets are redirected to 1.1.1.1 or 1.1.1.2 and IPv6 DNS packets are redirected to 1234::1 or 2345::1. You should remove the IP address to restore to the default values of the resolver.

With the default values of **208.67.222.222** and **208.67.220.220**, all DNS packets are redirected to Cisco Umbrella Anycast resolvers. The device uses the first default resolver IP address for all its redirection. When the Cisco device does not receive a response for three consecutive DNS queries, the device automatically switches to a different resolver IP address. This behavior remains the same for IPv6 resolver addresses.

Note IPv6 redirection is deferred and all IPV6 DNS packets are not redirected to Cisco Umbrella Anycast servers.

Public-key

Public-key is used to download the DNSCrypt certificate from Cisco Umbrella Integration cloud. This value is preconfigured to **B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79** which is the public-key of Cisco Umbrella Integration Anycast servers. If there is a change in the public-key and if you modify this command, then you have to remove the modified command to restore the default value. If you modify the value, the DNSCrypt certificate download may fail.

DNSCrypt

DNSCrypt is an encryption protocol to authenticate communications between the Cisco device and the Cisco Umbrella Integration. When the **parameter-map type umbrella** is configured and **umbrella out** is enabled on WAN interface, DNSCrypt gets triggered and a certificate is downloaded, validated, and parsed. A shared secret key is then negotiated, which is used to encrypt the DNS queries. For every hour this certificate is automatically downloaded and verified for an upgrade, a new shared secret key is negotiated to encrypt the DNS queries.

To disable DNSCrypt, use the **no dnscrypt** command and to re-enable DNSCrypt, use the **dnscrypt** command.

When the DNSCrypt is used, the DNS request packets size is more than 512 bytes. Ensure that these packets are allowed through the intermediary devices; otherwise, the response may not reach the intended recipients.

Verifying the Cisco Umbrella Connector Configuration

Verify the Cisco Umbrella Connector configuration using the following commands:

```
Router# show umbrella config
Umbrella Configuration
==================
   Token:  AAC1A2555C11B2B798FFF3AF27C2FB8F001CB7B2
   OrganizationID: 1882034
   Local Domain Regex parameter-map name: NONE
   DNSCrypt: Enabled
   Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

   UDP Timeout: 5 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
   Umbrella Interface Config:
       Number of interfaces with "opendns out" config: 1
         1. GigabitEthernet0/0/0
             Mode     :  OUT
             VRF      : global(Id: 0)
       Number of interfaces with "opendns in" config: 1
         1. GigabitEthernet0/0/1
             Mode      : IN
             Tag       : test
             Device-id : 010a6aef0b443f0f
             VRF       : global(Id: 0)

Device# show umbrella deviceid
Device registration details
Interface Name          Tag       Status   Device-id
GigabitEthernet0/0/1     guest  200 SUCCESS 010a7ba73bd216d1


Device#show umbrella dnscrypt
    DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
Last Successful Attempt : 10:55:40 UTC Apr 14 2016
Last Failed Attempt : 10:55:10 UTC Apr 14 2016
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
```

```
Minor Version : 0x0000
Query Magic : 0x717744506545635A
Serial Number : 1435874751
Start Time : 1435874751 (22:05:51 UTC Jul 2 2015)
End Time : 1467410751 (22:05:51 UTC Jul 1 2016)
Server Public Key :
ABA1:F000:D394:8045:672D:73E0:EAE6:F181:19D0:2A62:3791:EFAD:B04E:40B7:B6F9:C40B
Client Secret Key Hash :
BBC3:409F:5CB5:C3F3:06BD:A385:78DA:4CED:62BC:3985:1C41:BCCE:1342:DF13:B71E:F4CF
Client Public key :
ECE2:8295:2157:6797:6BE2:C563:A5A9:C5FC:C20D:ADAF:EB3C:A1A2:C09A:40AD:CAEA:FF76
NM key Hash :
F9C2:2C2C:330A:1972:D484:4DD8:8E5C:71FF:6775:53A7:0344:5484:B78D:01B1:B938:E884
```

```
Device# show umbrella deviceid detailed
Device registration details
 1.GigabitEthernet0/0/1
      Tag               : guest
      Device-id         : 010a6aef0b443f0f
      Description       : Device Id received successfully
      WAN interface     : GigabitEthernet0/0/0
      WAN VRF used      : global(Id: 0)
```

Show Commands

Show Commands at FP Layer

show platform software umbrella f0 local-domain Command

The **show platform software umbrella f0 local-domain** command displays all the local domains configured for Open DNS in the FP Layer.

```
Device# show platform software umbrella f0 local-domain
01. .*engineering.cisco.*
02. www.cisco.com
03. abc1
04. abc3
```

show platform software umbrella f0 config Command

The **show platform software umbrella f0 config** command shows whether the Umbrella global configurations performed at the control plane are propagated to the FP layer.

```
Device# show platform software umbrella f0 config
+++ Umbrella Config +++


Umbrella feature:
------------------
Init    : Enabled
Dnscrypt: Enabled

Timeout:
------------------
udp timeout: 5

Resolver config:
```

```
RESOLVER IP's
--------------------
208.67.220.220
208.67.222.222
2620:119:35::35
2620:119:53::53

Dnscrypt Info:

public_key    :
6A:1A:E6:1D:AE:9A:8A:52:4E:74:EC:8A:A2:57:B9:13:A4:73:33:95:70:8D:E9:9F:91:56:7B:64:B9:E0:FC:7D
magic_key     : 71 74 73 65 4A 61 49 70
serial number : 1463092899
```

show platform software umbrella f0 interface-info Command

The **show platform software umbrella f0 interface-info** command shows whether the Umbrella interface configurations performed at the control plane are propagated to the FP layer.

```
Device# show platform software umbrella f0 interface-info
Umbrella Interface Config:
InterfaceID           Name       Mode    DeviceID        Tag
-----------------------------------------------------------------
   06  GigabitEthernet0/0/0     OUT
   08  GigabitEthernet0/0/2      IN  010adb13752caabd  guest
   07  GigabitEthernet0/0/1      IN  010a0d9bfce516e3   test
```

Show Commands at CPP Layer

show platform hardware qfp active feature umbrella client config Command

The **show platform hardware qfp active feature umbrella client config** command displays the client configuration information at the CPP layer.

```
Device# show platform hardware qfp active feature umbrella client config
+++ Umbrella Config +++

Umbrella feature:

----------------

Init     : Enabled
Dnscrypt : Enabled

Timeout:

--------

udp timeout: 5

Orgid:

--------

orgid: 1892929

Resolver config:

------------------
```

```
RESOLVER IP's
 208.67.220.220
 208.67.222.222
 2620:119:53::53
 2620:119:35::35

Dnscrypt Info:

--------------

public_key   :
45:B1:D2:43:F9:A4:42:4A:B8:4E:CF:E7:5A:AE:CE:F2:81:43:F2:4F:E9:B9:7C:4D:6A:B5:90:93:07:9B:72:13
magic_key    : 71 31 56 77 44 57 30 6E
serial number: 1490391488

Umbrella Interface Config:

--------------------------

 08  GigabitEthernet0/0/1 :
      Mode     : OUT
```

Data Path Show Commands

show platform hardware qfp active feature umbrella datapath runtime Command

The **show platform hardware qfp active feature umbrella datapath runtime** command displays the runtime umbrella configuration in dataplane.

```
Device# show platform hardware qfp active feature umbrella datapath runtime
 udpflow_ageout: 5
 ipv4_count: 2
 ipv6_count: 2
 ipv4_index: 0
 ipv6_index: 0
 Umbrella IPv4 Anycast Address
 IP Anycast Address0: 208.67.220.220
 IP Anycast Address1: 208.67.222.222
 Umbrella IPv6 Anycast Address
 IP Anycast Address0: 2620:119:53:0:0:0:0:53
 IP Anycast Address1: 2620:119:35:0:0:0:0:35
 =DNSCrypt=
 key index: 0
 -key[0]-
  sn   : 1463092899
  ref        : 0
  magic      : 717473654a614970
  Client Public Key      :
ECE2:8295:2157:6797:6BE2:C563:A5A9:C5FC:C20D:ADAF:EB3C:A1A2:C09A:40AD:CAEA:FF76
  NM Key Hash            :
F9C2:2C2C:330A:1972:D484:4DD8:8E5C:71FF:6775:53A7:0344:5484:B78D:01B1:B938:E884
 -key[1]-
  sn   : 0
  ref cnt    : 0
  magic      : 0000000000000000
  Client Public Key      :
0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000
  NM Key Hash            :
0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000
```

show platform hardware qfp active feature umbrella datapath interface

The **show platform hardware qfp active feature umbrella datapath interface** command displays the interface configuration in datapath.

```
Device# show platform hardware qfp active feature umbrella datapath interface g0/0/0
uidb handle: 0xfff9
device id raw: 0x1, 0xa, 0x5b, 0x62, 0xc6, 0x5e, 0x6e 0xe7
```

show platform hardware qfp active feature umbrella datapath stats

The **show platform hardware qfp active feature umbrella datapath stats** command displays the Umbrella connector statistics in datapath.

```
Device# show platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats:
    Parser statistics:
      parser unknown pkt: 3867
      parser fmt error: 0
      parser count nonzero: 6
      parser pa error: 0
      parser non query: 0
      parser multiple name: 0
      parser dns name err: 0
      parser matched ip: 0
      parser umbrella redirect: 6
      local domain bypass: 0
      parser dns others: 0
      no device id on interface: 0
      drop erc dnscrypt: 0
      regex locked: 0
      regex not matched: 0
      parser malformed pkt: 0
    Flow statistics:
      feature object allocs : 6
      feature object frees  : 6
      flow create requests  : 6
      flow create successful: 6
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create failed, set aging : 0
      flow lookup requests  : 8
      flow lookup successful: 5
      flow lookup failed, CFT handle: 3
      flow lookup failed, getting FO: 0
      flow lookup failed, no match  : 0
      flow detach requests  : 6
      flow detach successful: 6
      flow detach failed, CFT handle: 0
      flow detach failed, getting FO: 0
      flow detach failed freeing FO : 0
      flow detach failed, no match  : 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow update requests  : 0
      flow update successful: 0
      flow update failed, CFT handle: 0
      flow update failed, getting FO: 0
      flow update failed, no match  : 0
```

```
DNSCrypt statistics:
bypass pkt: 4847
clear sent: 0
enc sent: 0
clear rcvd: 1
dec rcvd: 0
pa err: 0
enc lib err: 0
padding err: 0
nonce err: 0
flow bypass: 3
disabled: 9591
flow not enc: 5773
DCA statistics:
dca match success: 0
dca match failure: 8
```

Clear Command

clear platform hardware qfp active feature umbrella datapath stats

The **clear platform hardware qfp active feature umbrella datapath stats** command clears the Umbrella connector statistics in datapath.

```
Device# clear platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats Cleared
```

Troubleshooting Cisco Umbrella Integration

Troubleshoot issues that are related to enabling Cisco Umbrella Integration feature using these commands:

- **debug umbrella device-registration**
- **debug umbrella config**
- **debug umbrella dnscrypt**

Depending on the OS, run either of these two commands from the client device:

- The **nslookup -type=txt debug.umbrella.com** command from the command prompt of the Windows machine
- The **nslookup -type=txt debug.umbrella.com** command from the terminal window or shell of the Linux machine

```
nslookup -type=txt debug.opendns.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
debug.opendns.com text = "server r6.mum1"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 171.168.1.7"
debug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
```

```
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
debug.opendns.com text = "source 72.163.220.18:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

Configuration Examples

This example shows how to enable Cisco Umbrella Integration:

```
Device# configure terminal
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)# dnscrypt
Device(config-profile)# token AABBA59A0BDE1485C912AFE472952641001EEECC
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# umbrella in guest
Device(config)# interface gigabitEthernet 0/0/0
Device(config-if)# umbrella out
```

Deploying Cisco Umbrella Integration Using Cisco Prime CLI Templates

You can use the Cisco Prime CLI templates to provision the Cisco Umbrella Integration deployment. The Cisco Prime CLI templates make provisioning Cisco Umbrella Integration deployment simple.

Note The Cisco Prime CLI templates is supported only on Cisco Prime version 3.1 or later.

To use the Cisco Prime CLI templates to provision the Cisco Umbrella Integration deployment, perform these steps:

Step 1 Download the Cisco Prime templates corresponding to the Cisco IOS XE version running on your system.

Step 2 Unzip the file, if it is a zipped version.

Step 3 From Cisco Prime Web UI, choose **Configuration** > **Templates** > **Features and Technologies**, and then select **CLI Templates** (User Defined).

Step 4 Click **Import**.

Step 5 Select the folder where you want to import the templates and click Select Templates and choose the templates that you just downloaded.

Step 6 The following Cisco Umbrella Integration templates are available:

- Umbrella—Use this template to provision Umbrella Connector on the device.
- Umbrella Cleanup—Use this template to remove previously configured Umbrella Connector.

Cisco Umbrella Connector for iWAN DCA

Cisco Umbrella Connector for iWAN DCA features allows direct cloud access to applications and provides sufficient bandwidth for the best application performance. It directs only specified cloud applications out to local internet and sends the remaining traffic to central site for further security inspection for malware detection.

Direct Cloud Access Overview

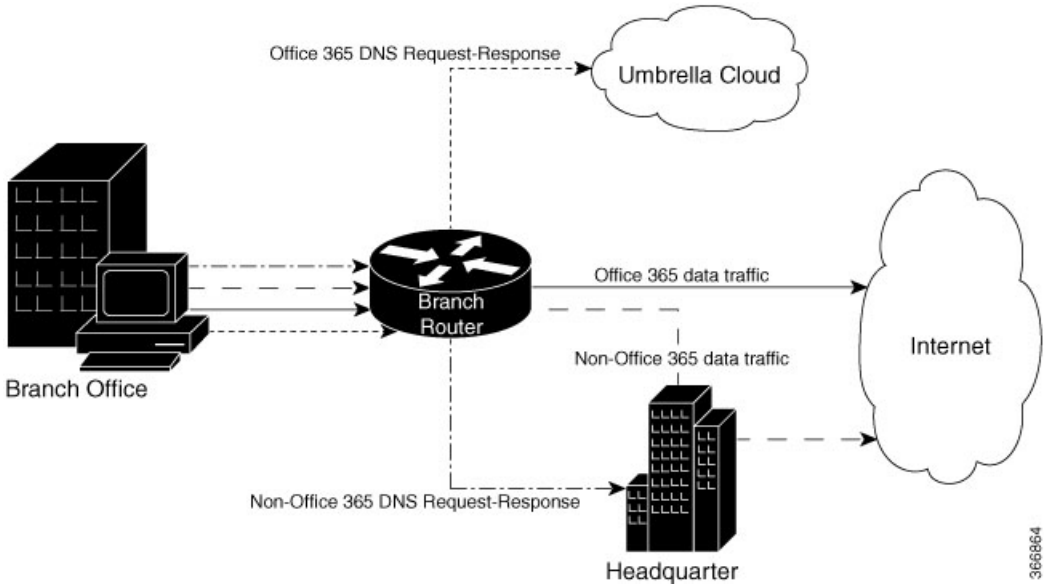
iWAN Direct Cloud Access (DCA) allows local breakout direct internet access for trusted domains. For security inspection, DCA directs specified cloud applications to the internet and the remaining traffic is sent to headquarters over VPN tunnel for malware detection, Data Loss Protection (DLP), application level accesses and so on.

Direct Cloud Access Architecture

The Direct Cloud Access feature allows you to address any security concerns as the local break-out DNS traffic is first sent to Umbrella Cloud for inspection to block any malicious cloud application. You can gain more security with DCA when you connect to your cloud services through secure and private connections. Business processes run faster through direct network access to the major cloud providers. A traffic classification mechanism is required in order to achieve direct internet access for selected cloud applications. DNS method is used to classify the Cloud SaaS applications.

The following figure explains the functionality of DCA for Office 365 Cloud Application:

Figure 2: DCA for Office 365



To achieve DCA functionality:

- Classify all the cloud applications based on the DNS.
- Intercept DNS traffic and make decisions based on the classification.

- If the traffic is from the interested cloud application then provide direct internet access. Ensure that security concerns are addressed for the breakout traffic.
- If the traffic is not from the interesting cloud application then pass it to the Headquarter for further security inspection and processing.

- Route HTTP, HTTPS data traffic to internet or headquarter depending on the above decision.

Direct Cloud Access Components

Direct Cloud Access feature has the following components:

- NBAR Classification
- Umbrella Connector
- Performance Routing

NBAR Classification

Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. NBAR uses several classification information metadata such as application name, ID, traffic class, business relevance, and so on.

For Direct Cloud Access feature, when NBAR recognizes the DNS traffic as belonging to cloud application, it attaches the traffic information to DNS packet so that the Umbrella Connector feature can extract and use the information.

Umbrella Connector

The Umbrella Connector is a component on the Cisco device that intercepts DNS traffic and redirects it to Umbrella cloud for security inspection and policy application.

If an Umbrella connector is configured to allow local breakout for cloud applications, it redirects DNS traffic from selected cloud applications. To configure an Umbrella Connector, intercept DNS packet and look for NBAR classification result attached to the packet. If a match is found, the packet is sent to the Umbrella cloud else the packet is forwarded to the enterprise DNS resolver.

Performance Routing (PfR)

Performance Routing (PfR) component delivers intelligent path control for application-aware routing across the WAN. Once a DNS response is received, the data traffic (HTTP, HTTPS etc.) originating from the cloud application is provided direct internet access (local break-out) or is hauled back to the headquarter for further security inspection by the PfR component.

Restrictions for Direct Cloud Access

This section describes the limitations and restrictions for this feature:

- DCA is not supported for IPv6 addresses.
- DCA is not supported if the DNS traffic do not go through the device (Umbrella interface where DCA is enabled).

- The Umbrella Connector does not provide local break-out support if applications directly access content, instead of using DNS resolution.
- DCA is not supported for DNS requests that do not have associated Network-Based Application Recognition (NBAR) result.
- From Umbrella Connector, local break out happens only at DNS level. Connector can not redirect non-DNS traffic.
- If an interface of the Umbrella Connector is configured to be in DCA mode, any local-domain bypass rules configured in the Umbrella global parameter-map will have no effect on DNS traffic through the interface.

Umbrella Connector Modes

Umbrella Connector operates in three modes:

- Umbrella Connector without DCA
- Umbrella Connector with DCA but no EDNS or DNSCrypt
- Umbrella Connector with DCA along with EDNS and DNSCrypt

How to Configure Direct Cloud Access

Configuring DCA involves two steps - defining a class map and a policy map.

Defining class-map

To define a match-all class map use the following command:

```
Router(config)# class-map match-all
```

The following is an example of defining a class map:

```
Router(config)# class-map match-all umbrella-direct-access
Router(config-cmap)# match protocol dns in-app-hierarchy
Router(config-cmap)# match protocol attribute application-set saas-apps office365
```

Defining policy-map

To define an Umbrella policy-map use the following command:

```
Router(config)# policy-map type umbrella
```

The following is an example of defining a umbrella policy map:

```
Router(config)# policy-map type umbrella umbrella-direct-access
Router(config-pmap)# class umbrella-direct-access
Router(config-pmap-c)# direct-cloud-access
```

Configuring Umbrella Connector on Interface

To configure Umbrella Connector on an interface, use the following commands:

```
Device(config-if)# umbrella in ?
WORD Umbrella interface tag
direct-cloud-access Umbrella direct cloud access

Device(config-if)# umbrella in direct-cloud-access ?
WORD Umbrella policy map name
default Umbrella direct cloud access with default policy

Device(config-if)# umbrella in direct-cloud-access policy ?
WORD Umbrella interface tag
```

The following is an example of interface command for Umbrella Connector with no Direct Cloud Access:

```
Device(config)# int g0/0/0
Device(config-if)# umbrella in guest
Device(config-if)#
Device # sh run | inc umbrella in
umbrella in guest
```

The following is an example of interface command for Umbrella Connector with Direct Cloud Access but no policy enforcement at cloud:

```
Router(config)# int g0/0/0
Router(config-if)# umbrella in direct-cloud-access umbrella-direct-access
```

The following is an example of interface command for Umbrella Connector with Direct Cloud Access with policy enforcement at cloud:

```
Router(config)# int g0/0/0
Router(config-if)# umbrella in direct-cloud-access umbrella-direct-access guest
```

Note **ip nbar protocol-discovery** interface command needs to be configured on the interfaces where umbrella in direct-cloud-access is configured for NBAR to classify DNS traffic.

High Availability Support

Cisco High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. With Cisco High Availability, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications.

The unique hardware and software architecture of the router is designed to maximize router uptime during any network event, and thereby provide maximum uptime and resilience within any network scenario. The

Cisco Umbrella Integration is enhanced to meet High Availability criteria on Cisco ASR 1000 Series platform. The Cisco ASR Series Router supports the following High Availability options:

- Dual IOSD
- Dual RP/FP
- Interchassis HA

Dual IOSD

In the dual IOSD scenario, the umbrella related configuration syncup happens automatically. However, the device registration and the DNSCrypt keys generation happens only on active IOSD processors. The configuration objects take the path from active device `iosd->fman-rp->fman-fp->cpp`. The standby IOSD is connected to backup **fman-rp** which is not connected to fman-fp. The objects from the standby **iosd/fman-rp** are in the standy **fman-rp** database.

Once the standby processor is active, the device registration and DNSCrypt keys exchange are enabled. The device-ID is same for both active and the standby processor. However, the DNSCrypt keys generated are different. When the active IOSD/fman-rp failsover, the newly active IOSD/fman-rp downloads the new keys to the CPP.

Any DNS response based on the old processor has the old key index so that it can be decrypted after the failover. Any DNS requests after the failover should start using the new keys seamlessly without any disruption. When the active router becomes unavailable for a reason, the standby router takes over the processing.

Note Dual IOSD feature is supported only on Cisco ASR 1002 and 1004 Series devices.

Dual RP/FP

In the multiple Route Processor (RP) and Forwarding Plane (FP) scenario, multiple RPs or FPs are available. The active RP is the one connecting to all the FPs and the standby-RP is idle. Only one RP and one FP are active at any time.

In the case of a FP-failover to a redundant FP, there is no disruption as the same objects based on the active RP are programmed on all the FPs and the redundant FP takes over seamlessly.

In the case of a RP failover, the active RP pushes all umbrella config objects along with new deviceid and dnscrypt key objects to active FP similar to dual IOSD processing.

Note Multiple RP and FP high availability feature is supported from Cisco ASR 1006 Series onwards.

Interchassis HA

The Interchassis High Availability feature is also known as the box-to-box redundancy feature. Interchassis High Availability enables the configuration of pairs of routers to act as backup for each other. This feature can be configured to determine the active router based on several failover conditions. When a failover occurs, the standby router seamlessly takes over and starts processing call signaling and performing media forwarding tasks.

You can configure pairs of devices to act as standbys for each other. Redundancy is configured on an interface basis. Pairs of redundant interfaces are known as redundancy groups (RGs). Redundancy occurs at an application level and does not require a complete physical failure of the interface or device for a switchover of the application to occur. When a switchover occurs, the application activity continues to run seamlessly on the redundant interface.

Redundant devices are joined by a configurable control link and a data synchronization link. The control link is used to communicate the status of devices. The data synchronization link is used to transfer stateful information from Network Address Translation (NAT) and the firewall and synchronize the stateful database. The pairs of redundant interfaces are configured with the same uniqueID number known as the redundant interface identifier (RII).

In the case of umbrella, the two devices independently register with the portal and get two unique device-IDs, generates two different DNSCrypt keys and pushes them to the CPP. Each of the device is operating independently as a stand alone device with the only modification to take care of asymmetric routing. When there is a failure in one of the chassis, the other chassis takes over. Note that since there is no syncup between devices, any messages received from the failed device cannot be decrypted on the active device. However, these messages can be encrypted with the keys of the new active chassis.

Note Interchassis HA feature is supported only on Cisco ASR 1001 to 1013 Series devices.

Additional References for Cisco Umbrella Integration

Related Documents

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

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 Cisco Umbrella Integration

Feature Name	Releases	Feature Information
Cisco Umbrella Integration	Cisco IOS XE Everest Release 16.6.1	The Cisco Umbrella Integration feature enables cloud-based security service by inspecting the DNS query that is sent to any DNS server through Cisco devices. The security administrator configures policies on the Umbrella cloud to either allow or deny traffic towards the fully qualified domain name (FQDN). This feature is supported only on Cisco ISRs.
Cisco Umbrella Connector for iWAN DCA	Cisco IOS XE Fuji Release 16.7.1	Umbrella Connector Infra Enablement for DCA is supported only on Cisco ISR 4000 Series.
Cisco Umbrella Connector for iWAN DCA	Cisco IOS XE Fuji Release 16.8.1	Umbrella Connector Infra Enablement for DCA is supported on Cisco ASR 1000 Series Routers, Cisco 1000 Series Integrated Services Routers and Cisco 4000 Series Integrated Services Routers.
High Availibility Support	Cisco IOS XE Gibraltar Release 16.10.1	Umbrella Connector for DCA with High Availability feature is supported only on Cisco ASR 1000 Series platform.