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 Cisco 1000 Series Integrated Services Routers (ISRs). The security administrator configures policies on the Cisco Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). Cisco 1000 Series ISR acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Cisco Umbrella portal.

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 the DNS server through Cisco 1000 Series Integrated Services Routers (ISR). The security administrator configures policies on the Umbrella cloud to either allow or deny traffic towards the fully qualified domain name (FQDN).

Prerequisites for Cisco Umbrella Integration

Before you configure the Cisco Umbrella Integration feature on the Cisco 1000 Series ISR, ensure that the following are met:

- The Cisco 1000 Series ISR has a security K9 license to enable Cisco Umbrella Integration.
- The Cisco 1000 Series ISR runs the Cisco IOS XE Everest 16.6.3 software image or later.
- Cisco Umbrella subscription license is available.
- The DNS traffic passed through the Cisco 1000 Series ISR.
- Communication for device registration to the Cisco Umbrella server is through 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

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.

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 Cisco 1000 Series ISRs. When a host initiates the traffic and sends a DNS query, the Cisco Umbrella Connector in Cisco 1000 Series ISR 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.

Encrypting the DNS Packet

The DNS packet sent from the Cisco 1000 Series ISR 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, Cisco 1000 Series ISR decrypts the packet and forwards it to the host.

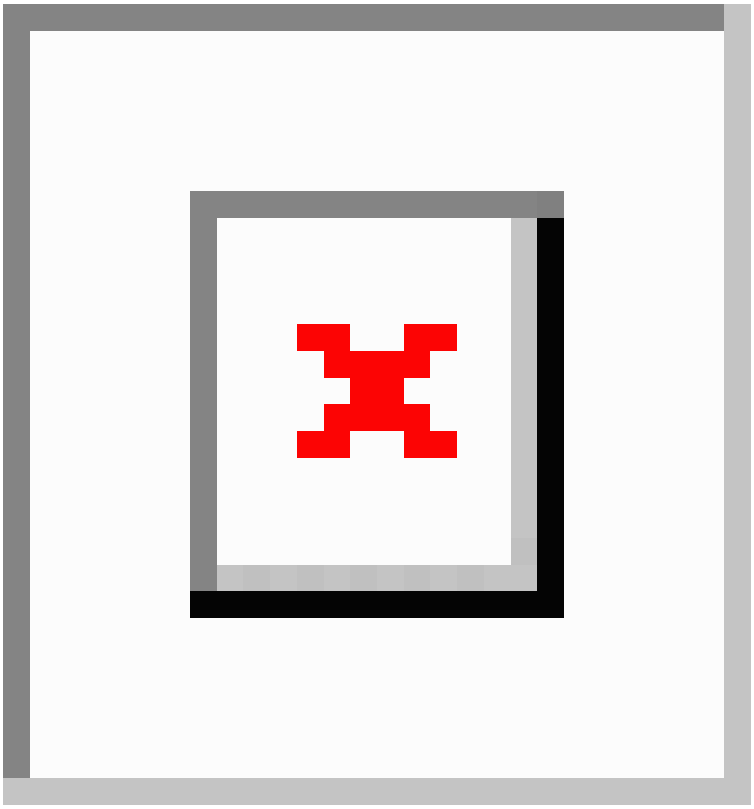
You can encrypt DNS packets only when the DNScrypt feature is enabled on the Cisco 1000 Series ISR.

Cisco 1000 Series ISR 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.

How to Configure Cisco Umbrella Connector

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
```

Register the Cisco Umbrella Tag

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

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

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

   ```
   interface vlan20
    umbrella in mydevice_tag
   ```

Note For Cisco 1000 Series ISRs, 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 Cisco 1000 Series ISR registers the tag to the Cisco Umbrella portal.

5. The Cisco 1000 Series ISR 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 Cisco 1000 Series ISR to successfully resolve the FQDN.

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

Configure Cisco 1000 Series ISR as a Pass-through Server

You can identify the traffic to be bypassed using domain names. In the Cisco 1000 Series ISR, you can define these domains in the form of regular expressions. If the DNS query that is intercepted by the Cisco 1000 Series ISR 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 umbrella global configuration as shown below:

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

Verify the Cisco Umbrella Connector Configuration

Verify the Cisco Umbrella Connector configuration using the following commands:

Show Commands

Show Commands at FP Layer

Show Commands at Cisco Packet Processor Layer

Data Path Show Commands

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
```

Troubleshoot the 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)"
```

When you deploy the Cisco Umbrella Integration feature:

- If you use the multiple EDNS options, DNS packets containing EDNS (DNSSEC) will not pass through the device. For assistance, contact Cisco Technical Support.
- If the WAN interface is down for more than 30 minutes, the device may reload with an exception. Disable the DNScrypt to stop this exception. For assistance, contact Cisco Technical Support .

Configuration Examples

This example shows how to enable Cisco Umbrella Integration on Cisco 1000 Series ISRs:

Deploy the 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:

Procedure

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 Cisco 1000 Series ISR.

- Umbrella Cleanup—Use this template to remove previously configured Umbrella Connector on Cisco 1000 Series ISR.

Additional References for Cisco Umbrella Integration

Related Documents

Related Topic	Document Title
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