Configuring 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). The Cisco switch acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Cisco Umbrella portal.

- Prerequisites for Cisco Umbrella Integration, on page 1
- Restrictions for Cisco Umbrella Integration , on page 1
- Information About Cisco Umbrella Integration, on page 2
- How to Configure Cisco Umbrella Integration, on page 8
- Configuration Examples for Cisco Umbrella Integration, on page 13
- Verifying the Cisco Umbrella Integration Configuration, on page 14
- Troubleshooting Cisco Umbrella Integration, on page 15
- Additional References for Cisco Umbrella Integration, on page 16
- Feature History for Cisco Umbrella Integration , on page 16

Prerequisites for Cisco Umbrella Integration

- Cisco Umbrella subscription license must be available. Go to https://umbrella.cisco.com/products/packages and click **Request a quote** to get the license.
- Communication for device registration to the Umbrella server is through HTTPS. This requires a root certificate to be installed on the device. You can download the certificate using this link: https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt.
- Get the API key, organization ID, and secret key or the token from the Cisco Umbrella registration server. You can download the certificate using this link: https://letsencrypt.org/certs/isrgrootx1.pem.

Restrictions for Cisco Umbrella Integration

- Cisco Umbrella Integration does not work in the following scenarios:
  - If an application or host uses IP address instead of DNS to query domain names.
  - If a client is connected to a web proxy and does not send DNS query to resolve the server address.

  - If DNS queries are generated by a Cisco Catalyst device.
  - If DNS queries are sent over TCP.
  - If DNS queries have record types other than address mapping and text.

- DNSv6 queries are not supported.
- DNS64 and DNS46 extensions are not supported.
- Extended DNS conveys only the IPv4 address of the host, and not the IPv6 address.
- Network Address Translation (NAT) is not supported on interfaces that has Cisco Umbrella enabled on it.
- The **umbrella in** and **umbrella out** commands cannot be configured on the same interface. Both these commands are not supported on the management interface and can be configured on a port basis only.
- DNS packet fragmentation is not supported.
- QinQ and Security Group Tag (SGT) packets are not supported.
- For Cisco Umbrella Active Directory Integration, if an interface does not have the **umbrella in** command enabled before a user is successfully authenticated, the username information is not sent with the DNS queries, and the default global policy may apply to such DNS queries.
- Cisco Umbrella registration and redirection can take place only on global virtual routing and forwarding (VRF). Connecting to the Umbrella server through any other VRF is not supported.
- Cisco Umbrella configuration commands can be configured only on L2, L3 physical ports, and switch virtual interfaces (SVIs). The commands cannot be configured on other interfaces such as port channels.

Information About Cisco Umbrella Integration

The following sections provide details about the Cisco Umbrella Integration feature.

Benefits of Cisco Umbrella Integration

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

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 a Cisco 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. The Umbrella Connector is a component in the Cisco device that intercepts DNS traffic and redirects it to the Cisco Umbrella cloud for security inspection and policy application. The Umbrella cloud is a cloud-based security service that inspects the queries received from Umbrella Connectors, and based on the Fully Qualified Domain Name (FQDN), determines if the content provider IP addresses should be provided or not in the response.

If the DNS query is for a local domain, the query is forwarded without changing the DNS packet to the DNS server in the enterprise network. The Cisco Umbrella Resolver inspects the DNS queries that are sent from an external domain. An extended DNS record that includes the device identifier information, organization ID, client IP address, and client username (in hashed form) is added to the query and sent to the Umbrella Resolver. Based on all this information, the Umbrella Cloud applies different policies to the DNS query.

The Cisco Umbrella Active Directory Connector retrieves and uploads user and group information mapping at regular intervals from the on-premises active directory to the Umbrella Resolver. On receiving DNS packets, the Umbrella Cloud applies the appropriate policy based on the preuploaded record of all the users and groups in the Umbrella Resolver. For more information on how to install the Cisco Umbrella Active Directory Connector, see the Active Directory Setup Guide.

Note

- Cisco Umbrella Active Directory Integration is configured by default if the Umbrella Connector is enabled on the device, and it does not need any additional commands to work.
- The Umbrella Connector automatically gets the username from the port-based authentication process and adds the username to every DNS query sent out by a user. For more information about port-based authentication process, see the chapter *Configuring IEEE 802.1x Port-Based Authentication*.

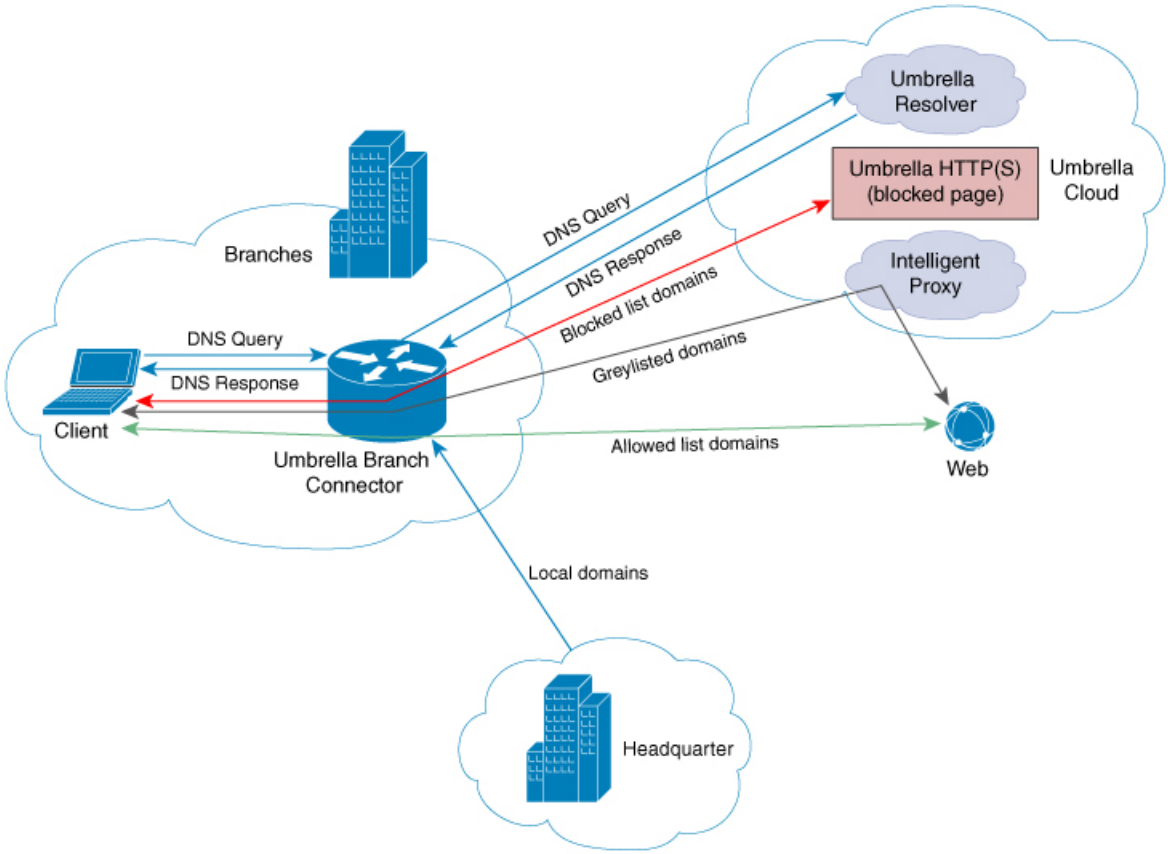
Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE support is mandatory for the Cisco Umbrella Active Directory Connector to work. For more information on how this integration works, see Active Directory Integration with Cisco ISE 2.x.

The Umbrella Integration Cloud might take one of the following actions based on the policies configured on the portal and the reputation of the DNS FQDN:

- Blocked list action: If the FQDN is found to be malicious or blocked by the customized enterprise security policy, the IP address of the Umbrella Cloud's blocked landing page is returned in the DNS response.
- Allowed list action: If the FQDN is found to be nonmalicious, the IP address of the content provider is returned in the DNS response.
- Greylist action: If the FQDN is found to be suspicious, the intelligent proxy unicast IP addresses are returned in the DNS response.

The following figure displays the traffic flow between the Umbrella Connector and the Umbrella Cloud:

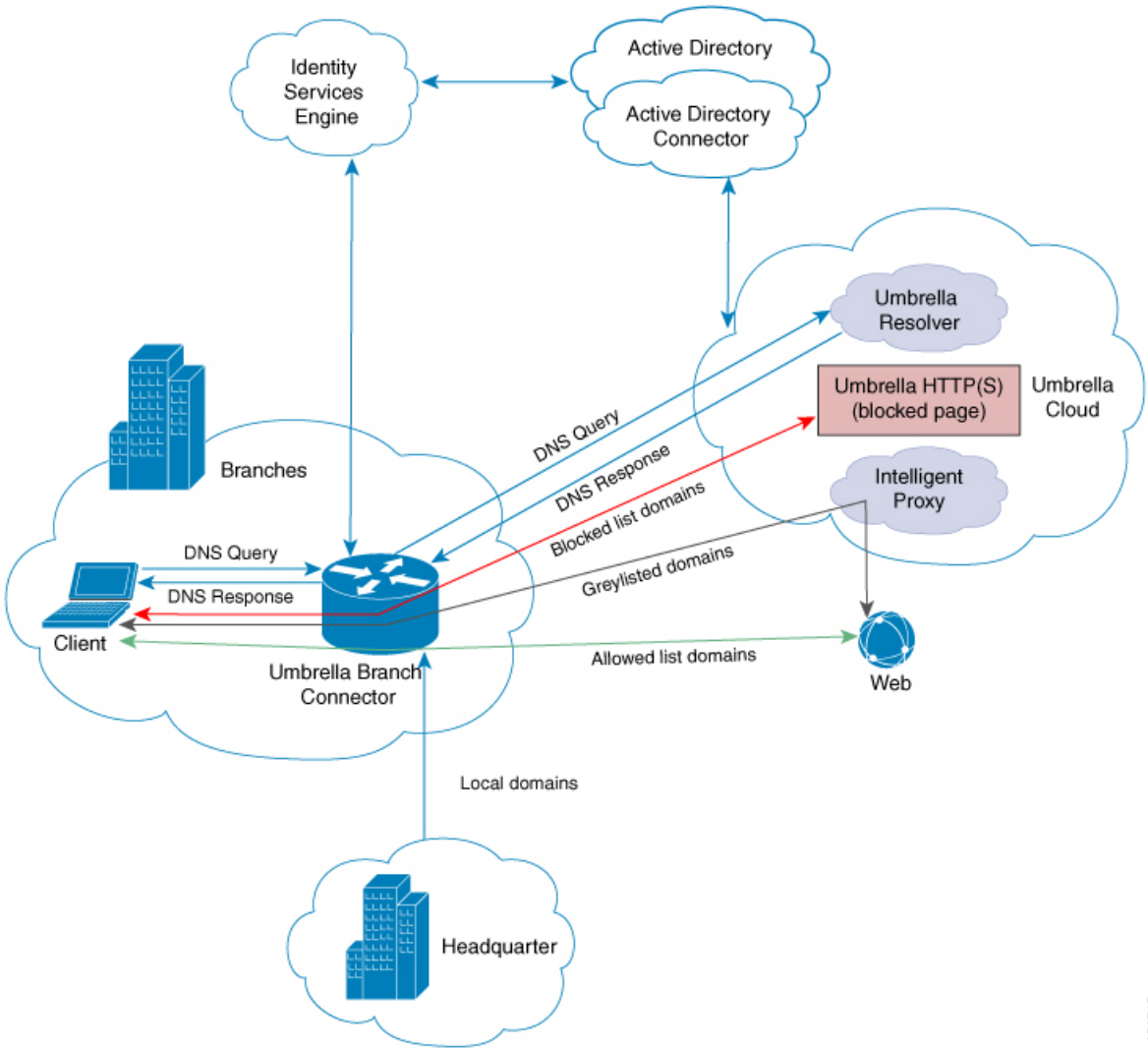
Figure 1: Cloud-Based Security Service Using Cisco Umbrella Integration



When the DNS response is received, the device forwards the response back to the host. The host extracts the IP address from the response, and sends the HTTP or HTTPS requests to this IP address. A hash of the username is sent in the DNS query as part of the EDNS record to the Umbrella servers.

The following figure displays the traffic flow between the Umbrella Connector, Cisco Identity Services Engine, the Umbrella Active Directory Connector, and the Umbrella Cloud:

Figure 2: Cloud-Based Security Service Using Cisco Umbrella Integration (with Cisco Identity Services Engine and Umbrella Active Directory Connector)



Handling of Traffic by Cisco Umbrella Cloud

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

- If the FQDN in the DNS query is malicious (falls under blocked listed domains), the 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 address, the Umbrella Cloud displays a page that informs a user that the requested page was blocked along with the reason for blocking.
- If the FQDN in the DNS query is nonmalicious (falls under allowed listed domains), the Umbrella Cloud returns the IP address of the content provider. The HTTP client sends the request to this IP address and gets the requested content.

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

Note One potential limitation in using an intelligent proxy unicast IP addresses is the probability of the datacenter going down when a client tries to send the traffic to the intelligent proxy unicast IP address. In this scenario, the client has completed DNS resolution for a domain that falls under the greylisted domain, and the client's HTTP or HTTPS traffic is sent to one of the obtained intelligent proxy unicast IP addresses. If that datacenter is down, the client has no way of knowing about it.

The Umbrella Connector does not act on the HTTP and HTTPS traffic, redirects any web traffic, or alter any HTTP or HTTPS packets.

DNS Packet Encyrption

DNS packets sent from a Cisco device to the Cisco Umbrella Integration server must be encrypted if the extended DNS 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, the device decrypts the packet and forwards it to the host.

Note

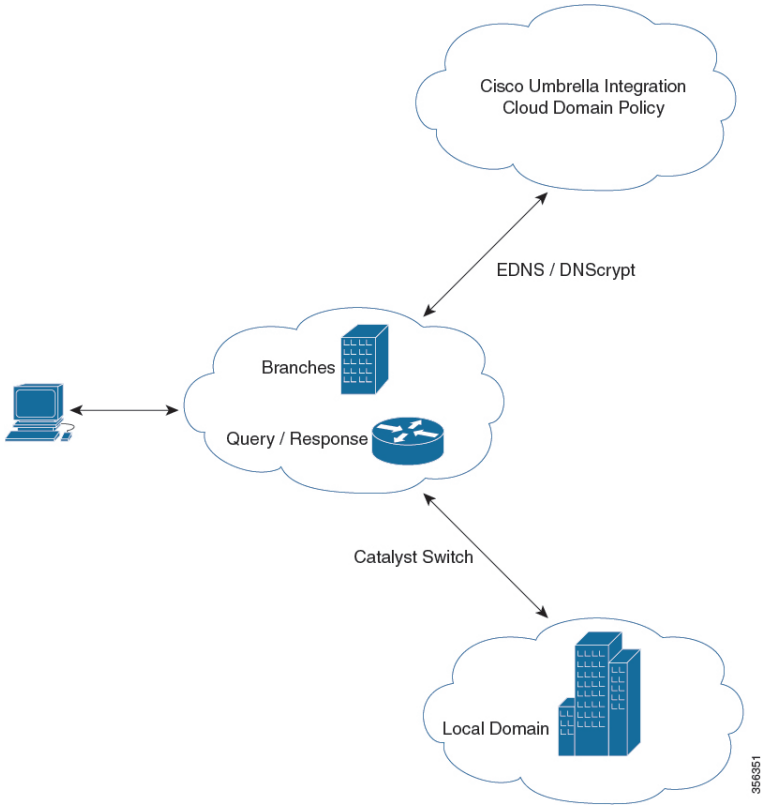
- You can encrypt DNS packets only when the DNScrypt feature is enabled on the Cisco device.
- The IP address of the client is exported to Umbrella Cloud for tracking statistics. We recommend that you do not disable DNScrypt because the IP will then be sent out unencrypted.

Cisco devices use the following Anycast recursive Cisco Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220

The following figure displays the Cisco Umbrella Integration topology.

Figure 3: Cisco Umbrella Integration Topology



DNSCrypt and Public Key

The following subsections provide detailed information about DNScrypt and Public Key.

DNSCrypt

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

When DNSCrypt is used, a DNS request packet's size is more than 512 bytes. Ensure that these packets are allowed through the intermediary devices. Otherwise, the response might not reach the intended recipients.

Enabling DNSCrypt on the device encrypts all DNS traffic. Subsequently, if DNS traffic inspection is enabled on an upstream firewall, in this case, Cisco Adaptive Security Appliance (ASA) firewall, the encrypted traffic cannot be inspected. As a result of this, DNS packets may be dropped by the firewall, resulting in DNS resolution failure. To avoid this, DNS traffic inspection must be disabled on upstream firewalls. For information about disabling DNS traffic inspection on the Cisco Adaptive Security Appliance (ASA) firewalls, see the *Cisco ASA Series Firewall CLI Configuration Guide*.

Public Key

Public key is used to download the DNSCrypt certificate from Umbrella 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 the Cisco Umbrella Integration Anycast servers. If there is a change in the public key, and if you modify the **public-key** command, you have to remove the modified command to restore the default value.

Caution If you modify the value, the DNSCrypt certificate download might fail.

The **parameter-map type umbrella global** command configures a parameter-map type in umbrella mode. When you configure a device using this command, the DNSCrypt and public key values are autopopulated.

We recommend that you change the **parameter-map type umbrella global** parameters only when you perform certain tests in the lab. If you modify these parameters, it can affect the normal functioning of the device.

Cisco Umbrella Registration

The Cisco Umbrella Connector can be registered using a token or an API-based authentication mechanism (a combination of the API key, organization ID, and secret key), which is issued by the Cisco Umbrella registration server. We recommend that you use the API method. If both the token and the API method are configured, the API method takes precedence over the token. The transition from token to API-based authentication is not seamless and a new device ID can be assigned to the same device during the transition. This impacts any device ID-specific policies that are configured on the Umbrella servers.

Cisco Umbrella Tag

Cisco Umbrella tags are used to configure the Cisco Umbrella Connector on an interface. Umbrella tags can be applied to specific DNS policies using the Umbrella Dashboard. These DNS policies are automatically applied to an Umbrella tag as long as the tag name matches a policy name, and are applicable only to clients that are connected through a specified interface. For information on how to create policies and associated options on the Umbrella server, see https://docs.umbrella.com/deployment-umbrella/docs/customize-your-policies-1.

Note

- All the interfaces can use the same Umbrella tag to form a uniform policy. Therefore, each interface does not require a unique Umbrella tag.
- If the Umbrella tag does not have a corresponding policy on the Umbrella server, the tag automatically defaults back to the global policy of that server.

How to Configure Cisco Umbrella Integration

The following sections provide information about the various tasks that comprise Cisco Umbrella integration.

Configuring the Umbrella Connector

Before you begin

- Have the root certificate establish the HTTPS connection with the Cisco Umbrella registration server. Import the root certificate of DigiCert into the device using the **crypto pki trustpool import terminal** command in global configuration mode. The following is a sample of the root certificate of DigiCert:

```
-----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 privacy-enhanced mail (PEM) import is successful. A confirmation message is displayed after you import the certificate.

Procedure

	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 umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Configures the parameter map type as umbrella mode, and enters parameter-map type inspect configuration mode.
Step 4	**dnscrypt** **Example:** `Device(config-profile)# dnscrypt`	Enables DNS packet encryption on the device.
Step 5	**token** *value* **Example:** `Device(config-profile)# token AABBA59A0BDE1485C912AFE472952641001EEECC`	Specifies the API token issued by the Cisco Umbrella registration server.
Step 6	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Registering the Cisco Umbrella Tag

Before you begin

- Configure the Umbrella Connector.
- Configure the **umbrella out** command before configuring the **umbrella in** command. Registration is successful only when port 443 is in Open state and allows the traffic to pass through the existing firewall.
- After you configure the **umbrella in** command with a tag, the device initiates the registration process by resolving api.opendns.com. Configure a name server by using the **ip name-server** command, and a domain lookup by using the **ip domain-lookup** command configured on the device to successfully resolve the FQDN.

Procedure

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Device(config)# interface gigabitEthernet 1/0/1`	Specifies the WAN interface, and enters interface configuration mode.
Step 4	**umbrella out** **Example:** `Device(config-if)# umbrella out`	Configures the Umbrella Connector on the interface to connect to the Umbrella Cloud servers.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode, and enters global configuration mode.
Step 6	**interface** *interface-type interface-number* **Example:** `Device(config)# interface gigabitEthernet 1/0/2`	Specifies the LAN interface, and enters interface configuration mode.
Step 7	**umbrella in** *tag-name* **Example:** `Device(config-if)# umbrella in mydevice_tag`	Configures the Umbrella Connector on the interface that is connected to the client. • The length of the Umbrella tag should not exceed 49 characters. • After you configure the **umbrella in** command with a tag, the device registers the tag to the Cisco Umbrella Integration server.
Step 8	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring a Cisco Device as a Pass-Through Server

You can identify the traffic that is to be bypassed by using domain names. You can define these domains in the form of regular expressions on a Cisco device. If the DNS query that is intercepted by the device matches one of the configured regular expressions, the query is bypassed to the specified DNS server without being redirected to the Umbrella Cloud.

Procedure

	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	**parameter-map type regex** *parameter-map-name* **Example:** `Device(config)# parameter-map type regex dns_bypass`	Configures a parameter-map type to match the specified traffic pattern, and enters parameter-map type inspect configuration mode.

Step 4	**pattern** *expression*
	Example:
	`Device(config-profile)# pattern www.cisco.com`
	`Device(config-profile)# pattern .*example.cisco.*`
		Configures a local domain or URL that is used to bypass the Umbrella Cloud.

Step 5	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 6	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Configures the parameter map type as umbrella mode, and enters parameter-map type inspect configuration mode.

	Command or Action	Purpose
Step 7	**token** *value* **Example:** `Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF`	Specifies the API token issued by the Cisco Umbrella registration server.
Step 8	**local-domain** *regex_param_map_name* **Example:** `Device(config-profile)# local-domain dns_bypass`	Attaches the regular expression parameter map with the Umbrella global configuration.
Step 9	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Configuration Examples for Cisco Umbrella Integration

The following sections provide Umbrella integration configuration examples.

Example: Configuring Cisco Umbrella Integration

The following example shows how to configure the Umbrella Connector and register the Umbrella tag:

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)# dnscrypt
Device(config-profile)# token AABBA59A0BDE1485C912AFE472952641001EEECC
Device(config-profile)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# umbrella out
Device(config-if)# exit
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# umbrella in mydevice_tag
Device(config-if)# exit
```

Example: Configuring a Cisco Device as a Pass-Through Server

The following example shows how to configure a Cisco device as a pass-through server:

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config-profile)# pattern www.cisco.com
Device(config-profile)# exit
```

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

Verifying the Cisco Umbrella Integration Configuration

Use the following commands in any order to view and verify the Cisco Umbrella Integration configuration.

The following is a sample output of the **show umbrella config** command:

```
Device# show umbrella config

Umbrella Configuration
=======================
   Token: 0C6ED7E376DD4D2E04492CE7EDFF1A7C00250986
   API-KEY: NONE
   OrganizationID: 2427270
   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 "umbrella out" config: 1
         1. GigabitEthernet1/0/48
             Mode     :  OUT
             VRF      : global(Id: 0)
       Number of interfaces with "umbrella in" config: 1
         1. GigabitEthernet1/0/1
             Mode       : IN
             DCA        : Disabled
             Tag        : test
             Device-id  : 010a2c41b8ab019c
             VRF        : global(Id: 0)

   Configured Umbrella Parameter-maps:
        1. global
```

The following is a sample output of the **show umbrella deviceid** command:

```
Device# show umbrella deviceid

Device registration details
Interface Name          Tag             Status          Device-id
GigabitEthernet1/0/1    guest           200 SUCCESS     010a2c41b8ab019c
```

The following is a sample output of the **show umbrella dnscrypt** command:

```
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
```

The following is a sample output of the **show umbrella deviceid detailed** command:

```
Device# show umbrella deviceid detailed

Device registration details
 1.GigabitEthernet1/0/2
      Tag               : guest
      Device-id         : 010a6aef0b443f0f
      Description       : Device Id received successfully
      WAN interface     : GigabitEthernet1/0/1
      WAN VRF used      : global(Id: 0)
```

The following is a sample output of the **show platform software dns-umbrella statistics** command. The command output displays traffic-related information, such as the number of queries sent, number of responses received, and so on.

```
Device# show platform software dns-umbrella statistics

=======================================
Umbrella Statistics
=======================================
Total Packets : 7848
DNSCrypt queries : 3940
DNSCrypt responses : 0
DNS queries : 0
DNS bypassed queries(Regex) : 0
DNS responses(Umbrella) : 0
DNS responses(Other) : 3906
Aged queries : 34
Dropped pkts : 0
```

Troubleshooting Cisco Umbrella Integration

You can troubleshoot issues related to the Cisco Umbrella Integration feature configuration by using the following commands.

Table 1: debug Commands for Cisco Umbrella Integration Feature

Command	Purpose
debug umbrella config	Enables Umbrella configuration debugging.

Command	Purpose
debug umbrella device-registration	Enables Umbrella device registration debugging.
debug umbrella dnscrypt	Enables Umbrella DNSCrypt encryption debugging.
debug umbrella redundancy	Enables Umbrella redundancy debugging.

From the command prompt of a Windows machine, or the terminal window or shell of a Linux machine, run the **nslookup -type=txt debug.opendns.com** command. The IP address that you specify with the **nslookup -type=txt debug.opendns.com** command must be the IP address of the DNS server.

```
nslookup -type=txt debug.opendns.com 10.0.0.1
Server: 10.0.0.1
Address: 10.0.0.1#53
Non-authoritative answer:
debug.opendns.com text = "server r6.xx"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 10.0.1.1"
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 10.1.1.1:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

Additional References for Cisco Umbrella Integration

Related Documents

Related Topic	Document Title
Security Commands	Command Reference, Cisco IOS XE Amsterdam 17.1.x (Catalyst 9200 Switches)

Feature History for Cisco Umbrella Integration

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.1.1	Cisco Umbrella Integration	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 Cisco Umbrella Cloud to either allow or deny traffic towards the FQDN.

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.3.1	Active Directory integration for Umbrella Connector	The Active Directory Connector retrieves and uploads user and group mapping at regular intervals from the on-premises active directory to the Umbrella Resolver.
Cisco IOS XE Cupertino 17.7.1	API Registration for Umbrella Switch Connector	API registration for the Umbrella Switch Connector can be done using an API key, an organization ID, and a secret key.
Cisco IOS XE Cupertino 17.9.1	Cisco Umbrella Integration	This feature was implemented on C9200CX-12P-2X2G, C9200CX-8P-2X2G, and C9200CX-12T-2X2G models of the Cisco Catalyst 9200CX Series Switches, which were introduced in this release.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.