Cisco Umbrella Integration

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History

Feature Name	Release Information	Description
Extended DNS (EDNS) and Local Domain Bypass Support with Cisco Umbrella Integration	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature enables cloud-based security service on Cisco vEdge devices by inspecting the DNS query. Once the DNS query is inspected, action is taken on it based on whether the query is for a local domain or an external domain.

- Overview of Cisco Catalyst SD-WAN Umbrella Integration, on page 2
- Restrictions for Umbrella Integration, on page 4
- Prerequisites for Umbrella Integration, on page 5
- Configure Cisco Umbrella Registration, on page 5
- Define Domain Lists, on page 6
- Configure Umbrella DNS Policy Using Cisco SD-WAN Manager, on page 6
- Attach DNS Umbrella Policy to Device Template, on page 7
- Upload Umbrella Root Certificates, on page 8
- Monitor Umbrella Feature, on page 8

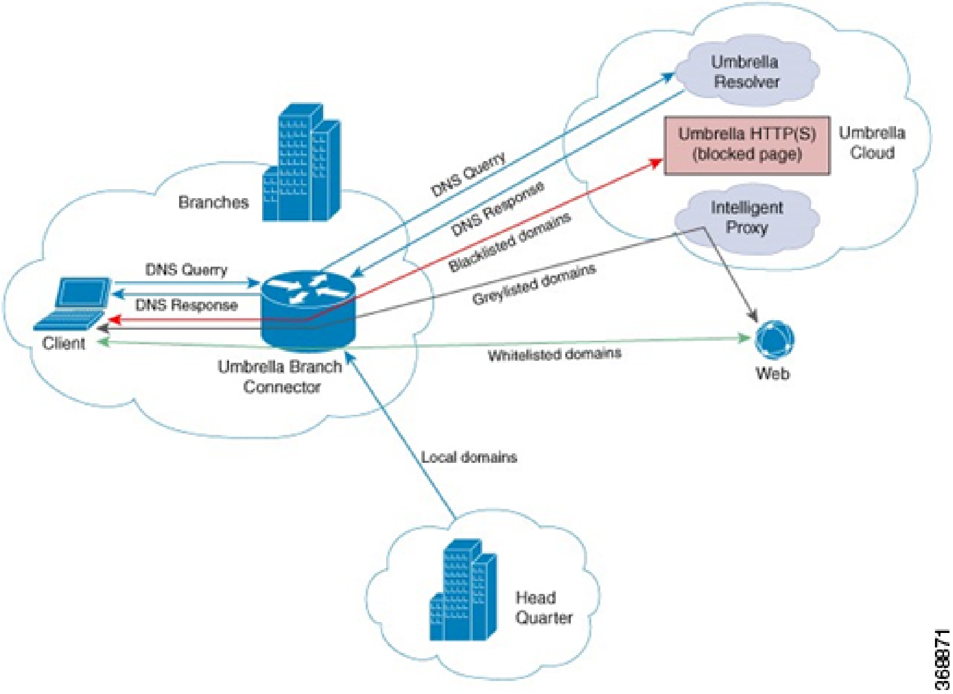
Overview of Cisco Catalyst SD-WAN Umbrella Integration

The Cisco Catalyst SD-WAN 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 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 Umbrella Resolver. An EDNS record includes the device identifier information, organization ID and client IP. Based on this information, 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 blocked 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 allowed list 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.

Figure 1: 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 Catalyst SD-WAN 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 blocked 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 allowedlisted 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.

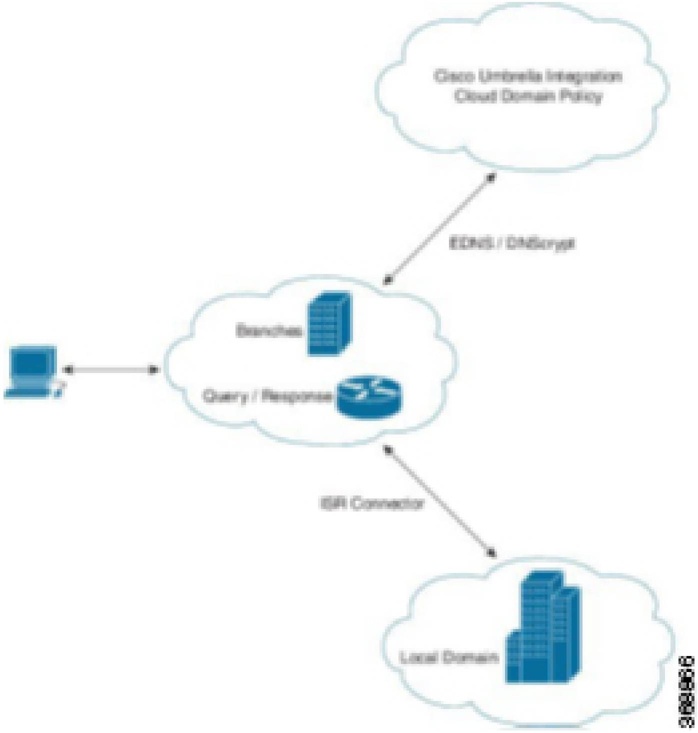
Encrypting the DNS Packet

The DNS packet sent from the device to 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 device.

The device uses the following Anycast recursive Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220

Figure 2: Umbrella Integration Topology



Restrictions for 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 device. In this case, the connector does not detect any DNS request and the connection to the web server bypasses any policy from the Umbrella portal.
- When the Umbrella Integration policy blocks a DNS query, the client is redirected to a Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Umbrella portal.
- The type A, AAAA, and TXT queries are the only records that are redirected. Other types of query bypasses the connector. Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to 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 under bypass list, and the allowed domain name length is 100 characters.
- Data-policy based NAT and Umbrella DNS redirect interoperability is not supported. If NAT for internet bound traffic is configured through a data policy instead of a default NAT route in service VPN, for Umbrella DNS redirection, you must create a rule to match the DNS request and then set action as

umbrella redirect. The data policy rule created for DNS redirect must be configured before the NAT rule in a sequence.

- Umbrella redirection does not work with DNS sent over TCP. Only UDP is supported.
- The Cisco Umbrella configuration may enforce IP address restrictions for the Service VPN configurations. If you do not follow the guidelines, configuration may result in traffic loss. For additional information about Cisco Umbrella configuration, see Cisco Umbrella SIG User Guide.

Prerequisites for Umbrella Integration

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

- The device has a security K9 license to enable Umbrella Integration.
- The device runs on Cisco SD-WAN Release 20.3.1 software image and later.
- Cisco Catalyst SD-WAN 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 device.

Configure Cisco Umbrella Registration

Use this procedure to configure Cisco Umbrella registration globally for all devices. The procedure retrieves the Umbrella registration parameters automatically.

When configuring individual policies, it is also possible to configure Umbrella registration, but it can be managed more flexibly using the following procedure:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Custom Options** and choose **Umbrella Registration**.
3. In the **Manage Umbrella Registration** dialog box, use one of the following methods to register devices to Umbrella. The registration details are used globally.
   - Cisco Umbrella Registration Key and Secret
     a. Click the **Get Keys** to retrieve Umbrella registration parameters automatically: Organization ID, Registration Key, and Secret.

Note To automatically retrieve registration parameters, Cisco SD-WAN Manager uses the Smart Account credentials to connect to the Umbrella portal. The Smart Account credentials are configured in Cisco SD-WAN Manager under **Administration** > **Settings** > **Smart Account Credentials**.

     b. (Optional) If the Umbrella keys have been rotated and the details that are automatically retrieved are incorrect, enter the details manually.
     c. Click **Save Changes**.

Define Domain Lists

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Custom Options**, and choose **Lists** from the drop-down menu.
3. Choose **Domain** in the left pane.
4. Click **New Domain List** to create a new domain list or click the domain name, and click the pencil icon on the right side for an existing list.
5. Enter the **Domain List Name**, **Add Domain**, and click **Add** to create the list.

Configure Umbrella DNS Policy Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. In the **Add Security Policy** wizard, click **Direct Internet Access**.
4. Click **Proceed**.
5. Click **Next** until you reach the **DNS Security** page.
6. From the **Add DNS Security Policy** drop-down list, choose one of the following:
    - **Create New**: A **DNS Security - Policy Rule Configuration** wizard is displayed.
    - **Copy from Existing**: Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
7. If you are creating a new policy using the **Create New** option, the **DNS Security - Policy Rule Configuration** wizard is displayed.
8. Enter a policy name in the **Policy Name** field.
9. The **Umbrella Registration Status** displays the status of the API Token configuration.
10. Click **Manage Umbrella Registration** to add a token, if you have not added one already.
11. Click **Match All VPN** to keep the same configuration for all the available VPNs and continue with Step 13.

    Or click **Custom VPN Configuration** if you need to add target service VPNs to your policy. A Target VPNs window appears, and continue with the next step.
12. To add target service VPNs, click **Target VPNs** at the top of the window.
13. Click **Save Changes** to add the VPN.
14. From the **Local Domain Bypass List** drop-down list, choose the domain bypass.
15. Click **Advanced** to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.
16. Click **Save DNS Security Policy**.

The **Configuration** > **Security** window is displayed, and the DNS policy list table includes the newly created DNS Security Policy.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

Table 2: DNS Security Policy

Field	Description
Add DNS Security Policy	From the **Add DNS Security Policy** drop-down list, select **Create New** to create a new DNS Security Policy policy. **Copy from Existing**: Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
Create New	Displays the DNS Security Policy wizard.
Policy Name	Enter a name for the policy.
Umbrella Registration Status	Displays the status of the API Token configuration.
Manage Umbrella Registration	Click **Manage Umbrella Registration** to add a token, if you have not added one already.
Match All VPN	Click **Match All VPN** to keep the same configuration for all the available VPNs.
Custom VPN Configuration	choose **Custom VPN Configuration** to input the specific VPNs.
Local Domain Bypass List	Choose the domain bypass.
DNS Server IP	Configure **DNS Server IP** from the following options: • **Umbrella Default** • **Custom DNS**
DNSCrypt	Enable or disable the DNSCrypt.
Next	Click **Next** to the policy summary page.

Attach DNS Umbrella Policy to Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Device Templates**, and choose **From Feature Template** from the Create Template drop-down menu.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the Device Model drop-down menu, choose a device.
4. Click **Additional Templates**. The screen scrolls to the **Additional Templates** section.
5. From the Security Policy drop-down menu, choose the name of the Umbrella DNS Security Policy you configured in the above procedure.
6. Click **Create** to apply the Umbrella policy to a device template.

Upload Umbrella Root Certificates

Minimum release: Cisco SD-WAN Release 20.9.1, Cisco vManage Release 20.9.1.

If edge devices in your Cisco Catalyst SD-WAN network require new Umbrella root certificates for Umbrella DNS security, you can upload an Umbrella root certificate bundle. The bundle contains a certificate for Cisco vEdge devices and a certificate for Cisco IOS XE Catalyst SD-WAN devices, in that order. After you upload the bundle, Cisco SD-WAN Manager pushes the appropriate certificates to the appropriate devices.

1. In the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit** in the **Umbrella DNS Certificate** row.
3. Perform one of the following actions to enter the Umbrella root certificate bundle in the **Umbrella Root Certificate** field:
   - Copy and paste the contents of the bundle. Ensure that the certificate for Cisco vEdge devices appears before the certificate for Cisco IOS XE Catalyst SD-WAN devices.
   - Click **Select a File** and navigate to and select the bundle that you want.
4. Click **Save**.

   Cisco SD-WAN Manager pushes the certificates to all devices that support an Umbrella root certificate.

Monitor Umbrella Feature

You can monitor the registered VPNs, DNSCrypt status, packet counts for required timestamps on an Umbrella configured router using the following steps.

To monitor the status of Umbrella DNS Configuration on a device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose the **Monitor** > **Network**.

2. Under Security Monitoring, click **Umbrella DNS Re-direct** in the left pane. **Umbrella DNS Re-direct** displays the number of packets that are redirected to configured DNS server.
3. Click **Local Domain Bypass** to view the number of packets that are bypassed from DNS server.