SD-WAN Umbrella Integration

The SD-WAN 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 Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). The router acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Umbrella cloud.

Overview of Cisco SD-WAN Umbrella Integration

The Cisco 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.

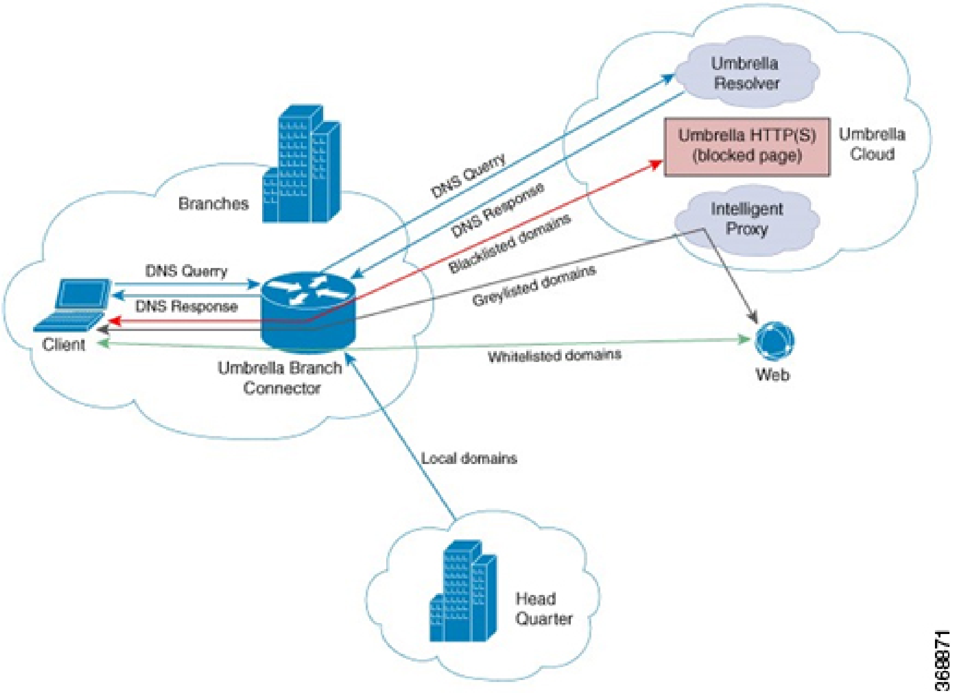
The Umbrella Integration cloud, based on the policies configured on the portal and the reputation of the DNS Fully Qualified Domain Name (FQDN) may take one of the following actions:

- 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 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.

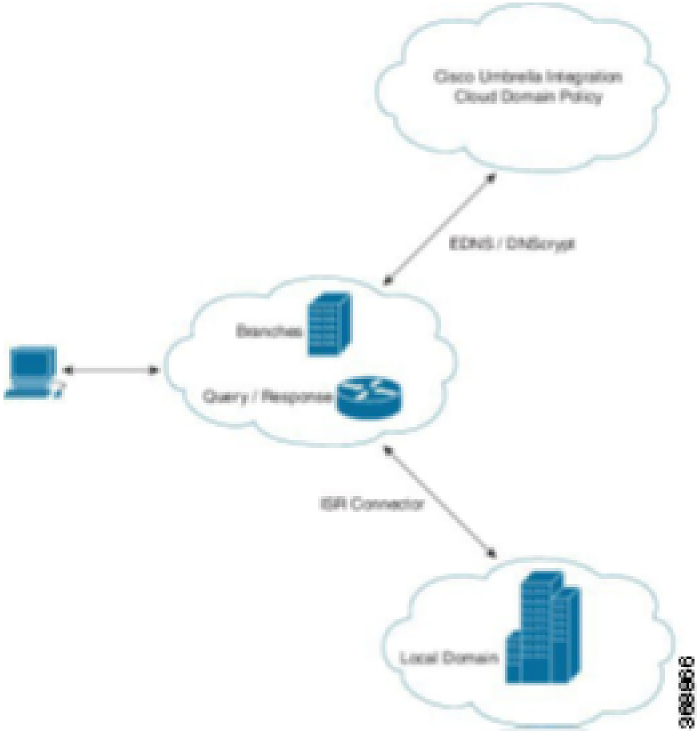
Encrypting the DNS Packet

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
- 2620:119:53::53
- 2620:119:35::35

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.

Prerequisites for Umbrella Integration

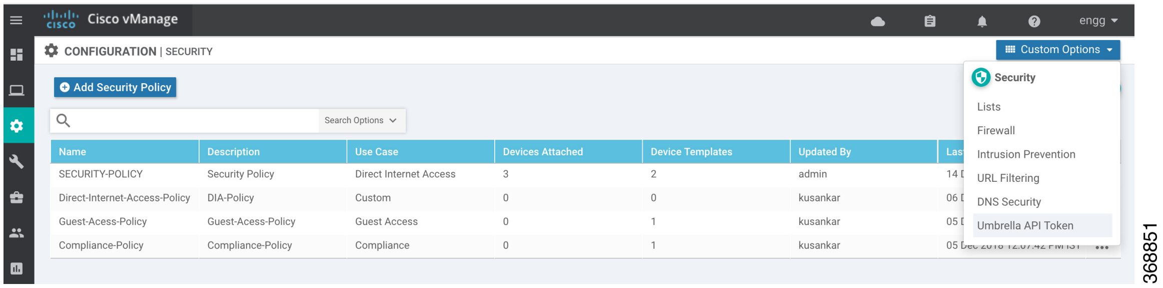
Before you configure the Umbrella Integration feature, ensure that the following are met:

- The device has a security K9 license to enable Umbrella Integration.
- The device runs on the SD-WAN IOS XE 16.10 software image or later.
- 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 Umbrella API Token

To configure Umbrella API token:

1. In Cisco vManage NMS, select the **Configuration** > **Security tab** > **Custom Options** on the right side to configure the Umbrella API.
2. Select **Umbrella API Token**.



Name	Description	Use Case	Devices Attached	Device Templates	Updated By	Las
SECURITY-POLICY	Security Policy	Direct Internet Access	3	2	admin	14 D
Direct-Internet-Access-Policy	DIA-Policy	Custom	0	0	kusankar	06 D
Guest-Acess-Policy	Guest-Acess-Policy	Guest Access	0	1	kusankar	05 D
Compliance-Policy	Compliance-Policy	Compliance	0	1	kusankar	05 Dec 2018 12:07:42 PM IST

3. Enter token number in the **Umbrella Token** field.

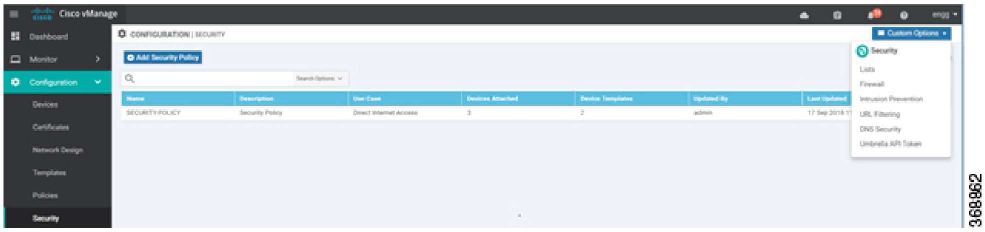
Note Must be exactly 40 hexadecimal.

4. Click **Save Changes**to configure the Umbrella API Token.

Define Domain Lists

To define Domain-List, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the **Configuration** > **Security tab** > **Custom Options** in the right side.



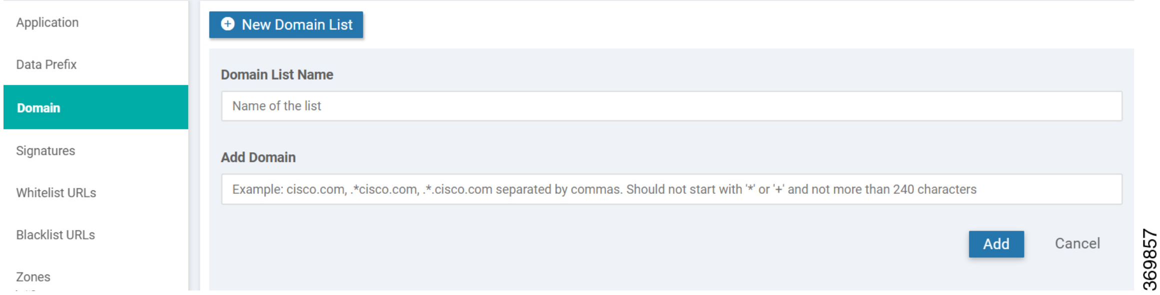
Name	Description	Use Case	Devices Attached	Device Templates	Updated By	Last Updated
SECURITY-POLICY	Security Policy	Direct Internet Access	3	2	admin	17 Sep 2018 1

2. Click on **Lists** in the Custom Options drop-down.

3. Select **Domain** from the left pane.

4. Click on **New Domain List** to create a new domain list or select the domain name and click on pencil icon on the right side for the existing list.

5. Enter the **Domain List Name, Add Domain** and click **Add** to create the



Domain List Name

Name of the list

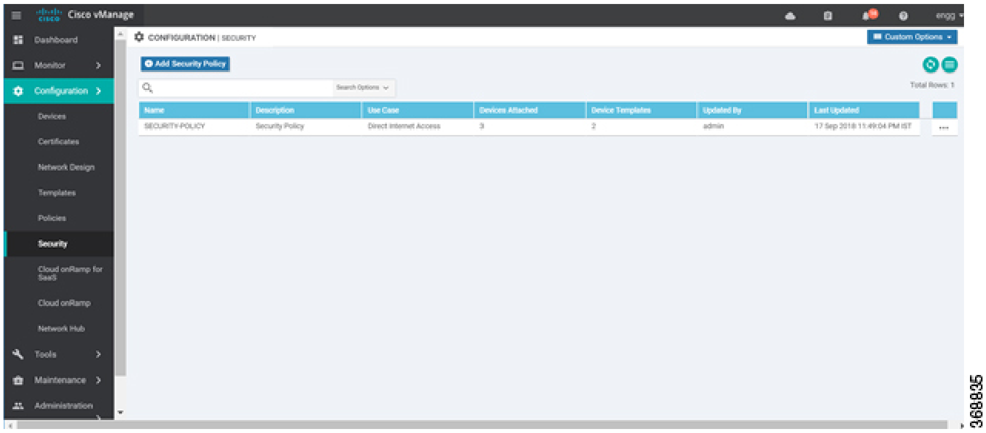
Add Domain

Example: cisco.com, .*cisco.com, .*.cisco.com separated by commas. Should not start with '*' or '+' and not more than 240 characters

Configure Umbrella DNS Policy Using vManage

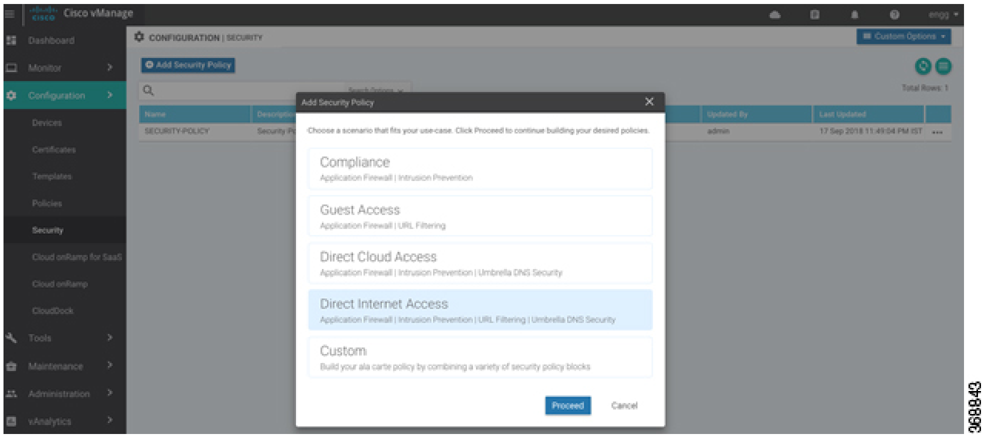
To configure umbrella through DNS Security:

1. In Cisco vManage NMS, select the **Configuration** > **Security** tab in the left side panel.



Name	Description	Use Case	Devices Attached	Device Templates	Updated By	Last Updated
SECURITY-POLICY	Security Policy	Direct Internet Access	3	2	admin	17 Sep 2018 11:49:04 PM IST

2. Click **Add Security Policy**. The Add Security Policy wizard appears.



Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

Compliance
Application Firewall | Intrusion Prevention

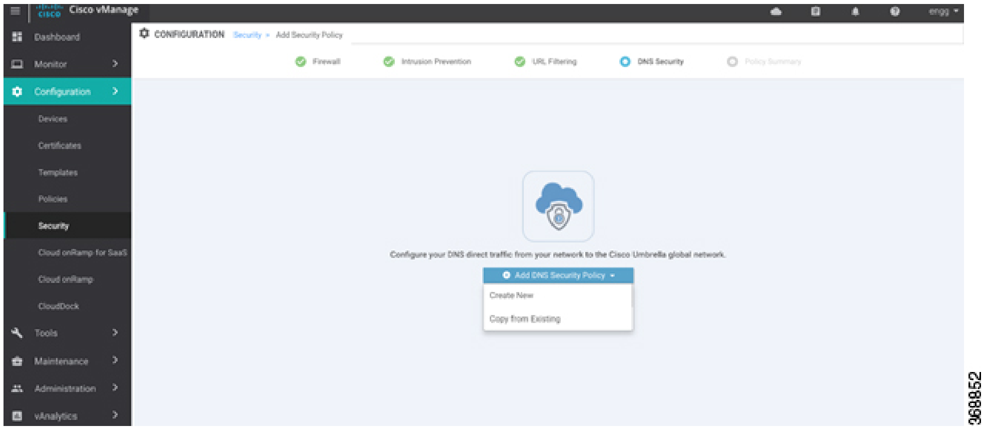
Guest Access
Application Firewall | URL Filtering

Direct Cloud Access
Application Firewall | Intrusion Prevention | Umbrella DNS Security

Direct Internet Access
Application Firewall | Intrusion Prevention | URL Filtering | Umbrella DNS Security

Custom
Build your ala carte policy by combining a variety of security policy blocks

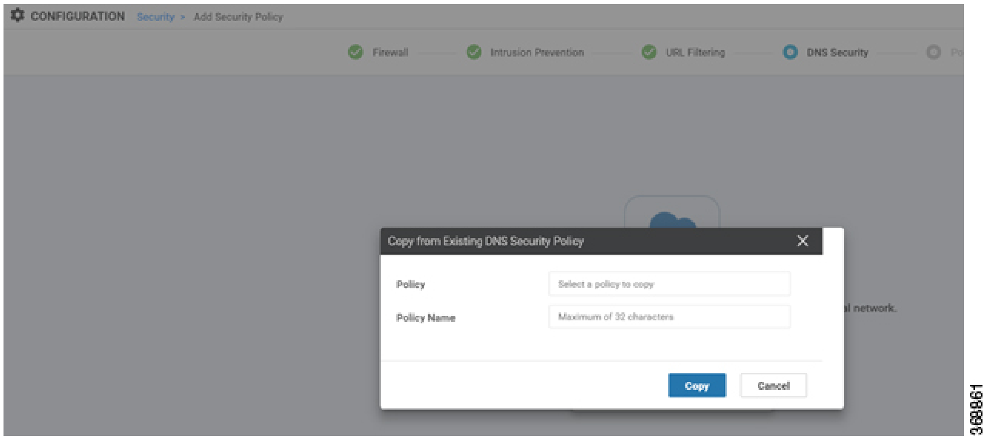
3. The Add Security Policy configuration wizard opens, and various use-case scenarios display.
4. In Add Security Policy, select **Direct Internet Access**.
5. Click **Proceed** to add an Umbrella DNS Security policy in the wizard.
6. In the Add Security Policy wizard, select **DNS Security** tab to create a new DNS Security policy.



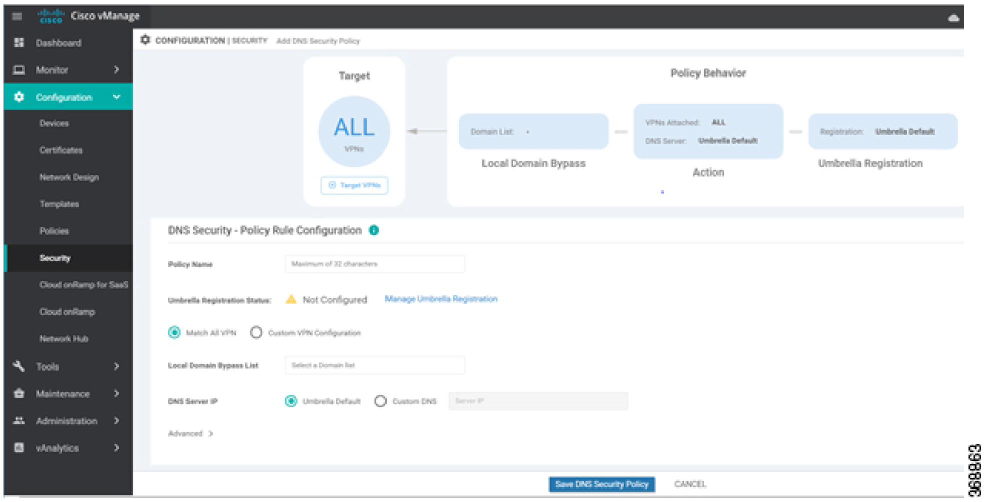
Configure your DNS direct traffic from your network to the Cisco Umbrella global network.

7. Click the **Add DNS Security Policy** drop-down and select from the following options:

   - Create New - A DNS Security - Policy Rule Configuration wizard appears and continue with Step 8.
   - Copy from Existing - A Copy from Existing DNS Security Policy wizard appears. Select a **Policy** from the drop-down and enter **Policy Name** and copy the policy to a device.



8. If you are creating a new policy using **Create New**, a DNS Security - Policy Rule Configuration wizard appears.



Domain List: -

VPNs Attached: ALL
DNS Server: Umbrella Default

Registration: Umbrella Default

DNS Security - Policy Rule Configuration

Policy Name: Maximum of 32 characters

Umbrella Registration Status: Not Configured Manage Umbrella Registration

● Match All VPN ○ Custom VPN Configuration

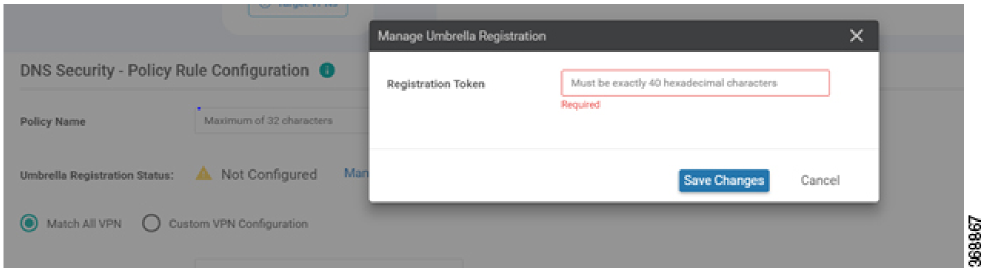
Local Domain Bypass List: Select a Domain list

DNS Server IP: ● Umbrella Default ○ Custom DNS Server IP

9. Enter a policy name in the **Policy Name** field.

10. The Umbrella Registration Status displays the status about the API Token configuration.

11. Click on **Manage Umbrella Registration** to add a token.


Target VPNs
DNS Security - Policy Rule Configuration
Manage Umbrella Registration
Save Changes
Cancel
368867

Policy Name: Maximum of 32 characters

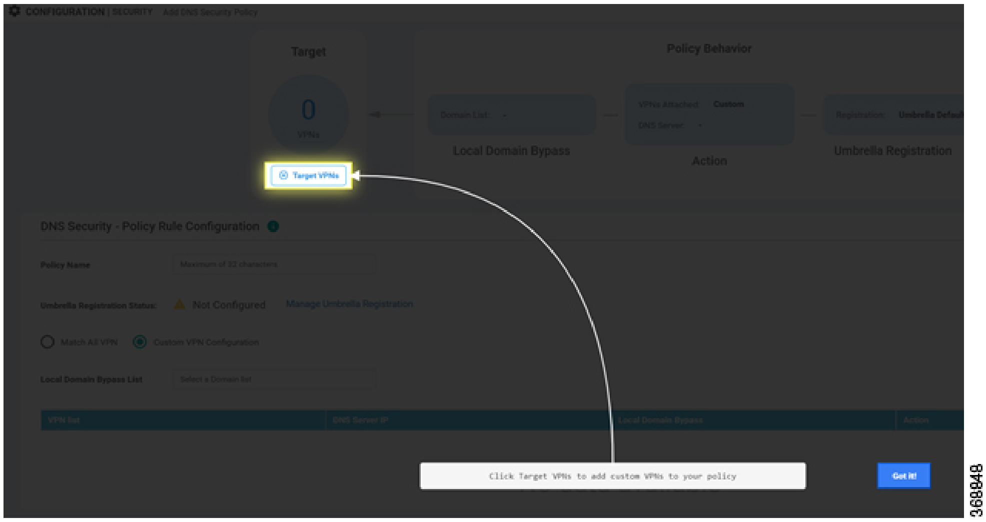
Umbrella Registration Status: Not Configured Man

● Match All VPN ○ Custom VPN Configuration

Registration Token: Must be exactly 40 hexadecimal characters
Required

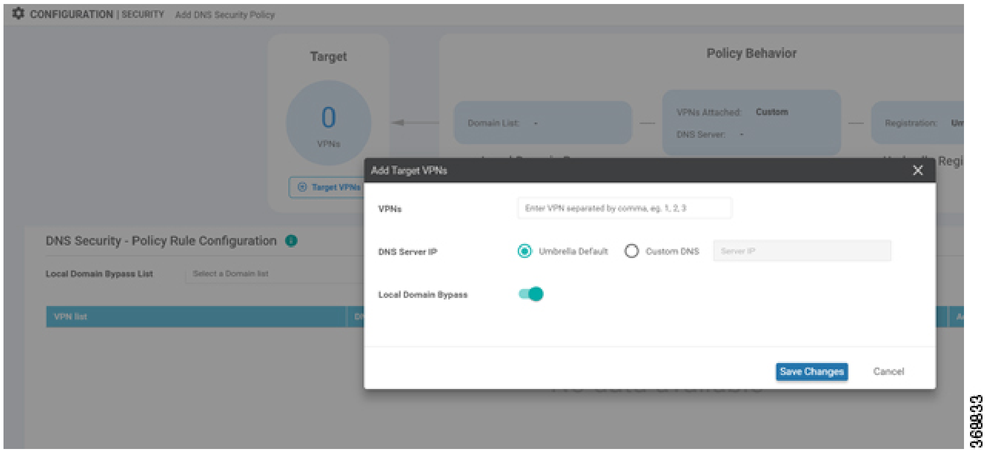
12. Select **Match All VPN** option if you need to keep the same configuration for all the available VPNs and continue with Step 13.

    Or select **Custom VPN Configuration** if you need to add target VPNs to your policy. A Target VPNs wizard appears.



Click Target VPNs to add custom VPNs to your policy

13. To add target VPNs, click **Target VPNs** in the Add DNS Security Policy wizard.

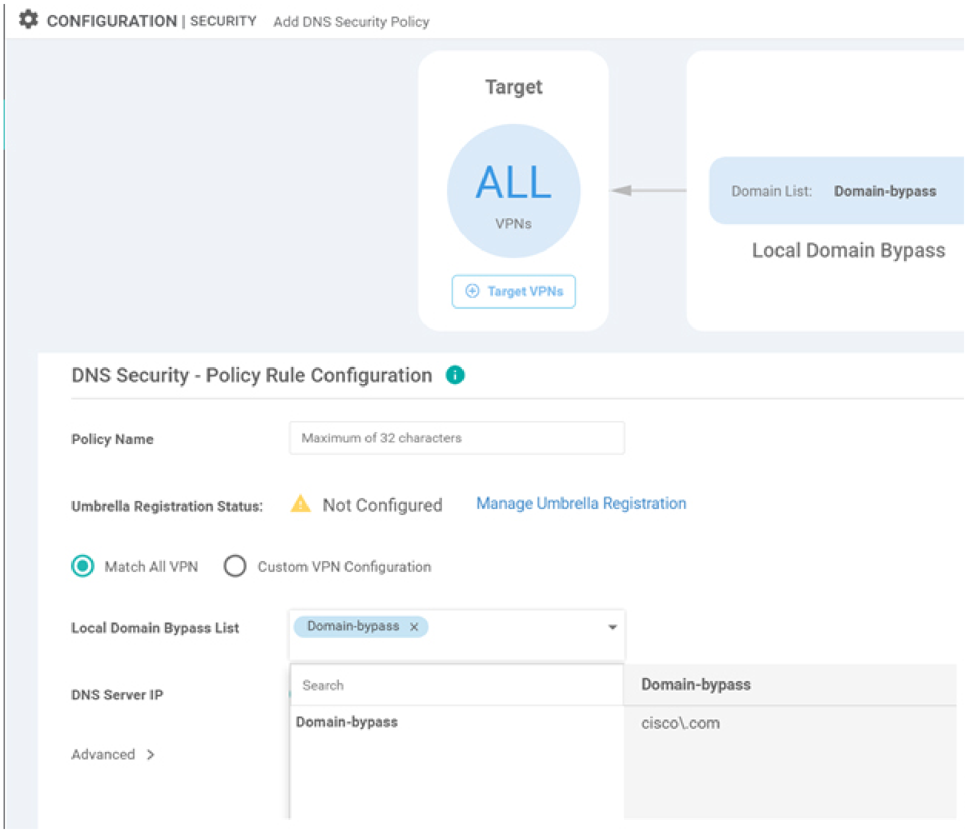


DNS Server IP ● Umbrella Default ○ Custom DNS

Local Domain Bypass

14. Click **Save Changes** to add the VPN.

15. Select the domain bypass from the **Local Domain Bypass List** drop-down as shown.


CONFIGURATION | SECURITY Add DNS Security Policy
Target
ALL
VPNs
Target VPNs
Domain List: Domain-bypass
Local Domain Bypass

DNS Security - Policy Rule Configuration

Policy Name: Maximum of 32 characters

Umbrella Registration Status: ⚠ Not Configured Manage Umbrella Registration

● Match All VPN ○ Custom VPN Configuration

Local Domain Bypass List: Domain-bypass ×

DNS Server IP

Advanced >

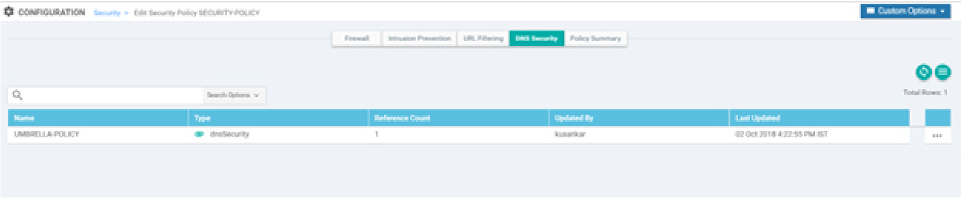
Search	Domain-bypass
Domain-bypass	cisco\.com

368860

16. Configure the **DNS Server IP** from the following options:
    - Umbrella Default
    - Custom DNS

17. Click on the **Advanced** tab to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.

18. Click **Save DNS Security Policy** to configure DNS Security policy. The **Configuration** > **Security** screen is then displayed, and the DNS Policy list table includes the newly created DNS Security Policy.



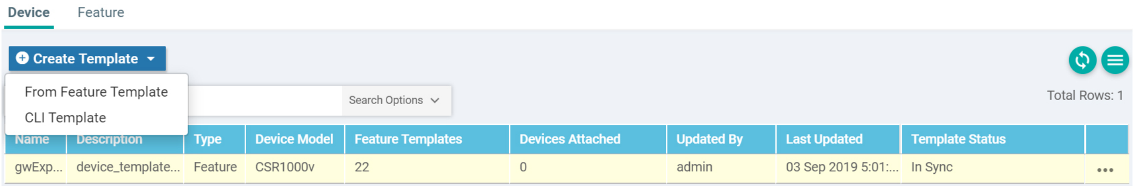
Name	Type	Reference Count	Updated By	Last Updated
UMBRELLA-POLICY	dnsSecurity	1	kusankar	02 Oct 2018 4:22:55 PM IST

368834

Apply DNS Umbrella Policy to an IOS XE Router

To apply DNS Umbrella Policy:

1. In vManage NMS, select the **Configuration** > **Templates** screen.



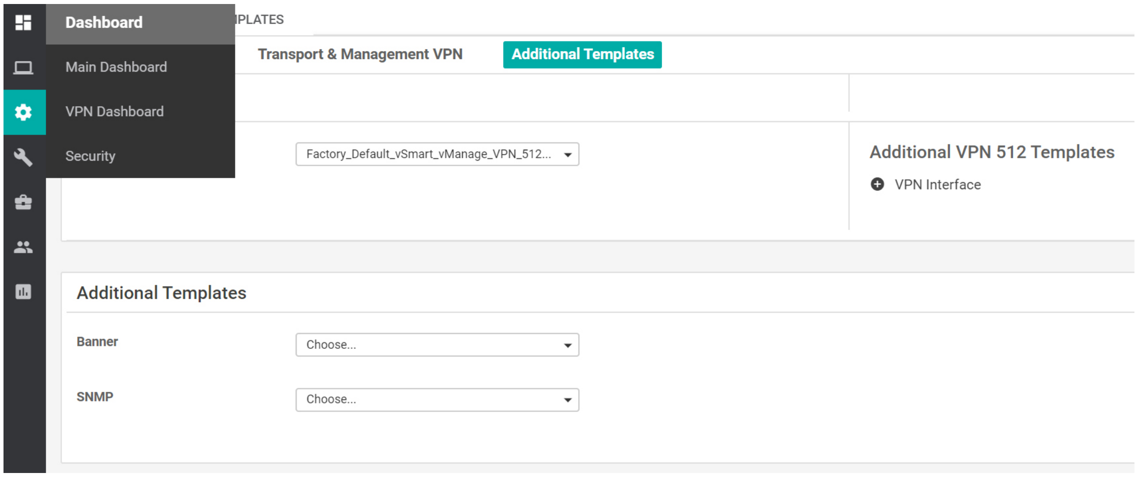
Total Rows: 1

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
gwExp...	device_template...	Feature	CSR1000v	22	0	admin	03 Sep 2019 5:01:...	In Sync	•••

2. In the **Device** tab, select **From Feature Template** from the Create Template drop-down,.

3. From the Device Model drop-down, select one of the IOS XE devices.

4. Click the **Additional Templates** tab. The screen scrolls to the **Additional Templates** section.



Factory_Default_vSmart_vManage_VPN_512...

Additional Templates

Banner: Choose...

SNMP: Choose...

5. From the Security Policy drop-down, select the name of the Umbrella DNS Security Policy you configured in the above procedure.

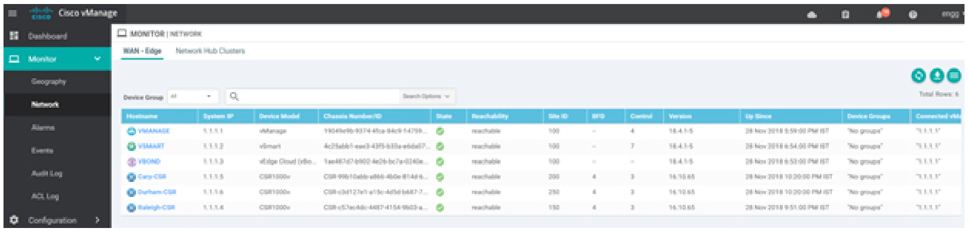
6. Click **Create** to apply Umbrella policy to a device.

Monitoring Umbrella Feature

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

To monitor the status of Umbrella DNS Configuration on IOS XE device:

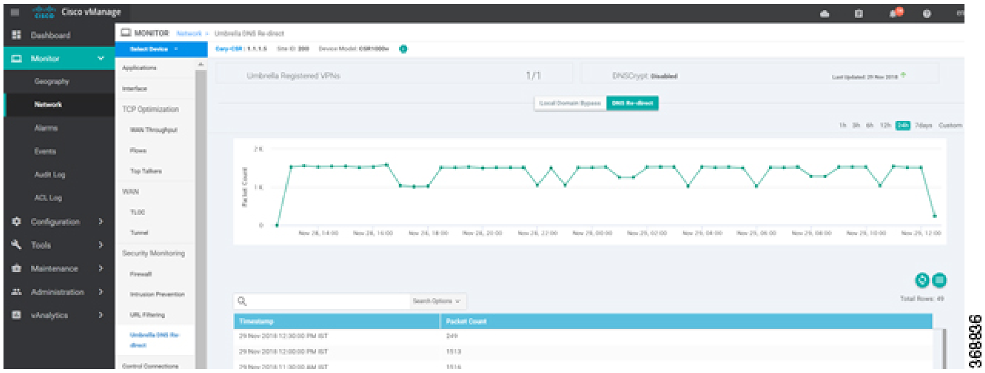
1. From the **Monitor** > **Network** screen, select an IOS XE device.



Total Rows: 6

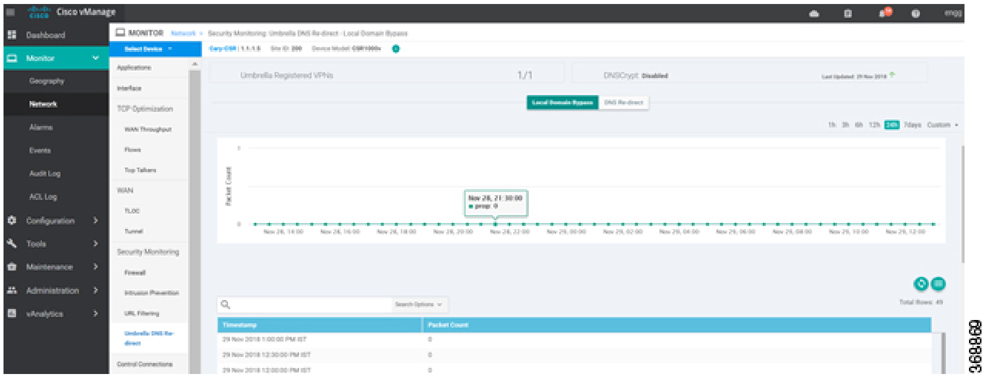
Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	Version	Up Since	Device Groups	Connected vMa
VMANAGE	1.1.1.1	vManage	19049e9b-9374-4fca-84c9-14759...	✓	reachable	100	–	4	18.4.1-5	28 Nov 2018 5:59:00 PM IST	"No groups"	"1.1.1.1"
VSMART	1.1.1.2	vSmart	4c25abb1-eae3-43f5-b35a-e6da07...	✓	reachable	100	–	7	18.4.1-5	28 Nov 2018 6:54:00 PM IST	"No groups"	"1.1.1.1"
VBOND	1.1.1.3	vEdge Cloud (vBo...	1ae487d7-b902-4e26-bc7a-0240e...	✓	reachable	100	–	–	18.4.1-5	28 Nov 2018 6:53:00 PM IST	"No groups"	"1.1.1.1"
Cary-CSR	1.1.1.5	CSR1000v	CSR-99b10abb-a866-4b0e-814d-6...	✓	reachable	200	4	3	16.10.65	28 Nov 2018 10:20:00 PM IST	"No groups"	"1.1.1.1"
Durham-CSR	1.1.1.6	CSR1000v	CSR-c3d127e1-a15c-4d5d-b687-7...	✓	reachable	250	4	3	16.10.65	28 Nov 2018 10:20:00 PM IST	"No groups"	"1.1.1.1"
Raleigh-CSR	1.1.1.4	CSR1000v	CSR-c57ec4dc-4487-4154-9b03-a...	✓	reachable	150	4	3	16.10.65	28 Nov 2018 9:51:00 PM IST	"No groups"	"1.1.1.1"

2. In the left panel, under Security Monitoring, select **Umbrella DNS Re-direct** tab. The Umbrella DNS Re-direct wizard displays showing how many packets are redirected to configured DNS server.



Timestamp	Packet Count
29 Nov 2018 12:30:00 PM IST	249
29 Nov 2018 12:00:00 PM IST	1513
29 Nov 2018 11:30:00 AM IST	1516

3. Click on **Local Domain Bypass** to monitor the packet counts showing how many packets are bypassed to DNS server.



Timestamp	Packet Count
29 Nov 2018 1:00:00 PM IST	0
29 Nov 2018 12:30:00 PM IST	0
29 Nov 2018 12:00:00 PM IST	0

Umbrella Integration Using CLI

Configure the Umbrella Connector

Communication for device registration to the Cisco Umbrella server is via HTTPS. This requires a DigiCert root certificate which is auto installed on the router by default.

To configure Umbrella Connector:

- Get the API token from the Umbrella portal.
- Define VRFs and each VRF can has two options: DNS resolver and enabling local domain list.
    - Umbrella registration is done per VRF only if DNS resolver is configured as Umbrella.
    - Local domain bypass list is global and each VRF can enable or disable the local domain bypass list. If enabled, the DNS packet will be matched against the local domain list.
- Umbrella is a Direct Internet Access (DIA) feature, so NAT configuration is mandatory.

Sample configuration:

```
Device# config-transaction
    Device(config)# parameter-map type umbrella global
    Device(config-profile)#?
    parameter-map commands:
          dnscrypt          Enable DNSCrypt
          exit              Exit from parameter-map
          local-domain      Local domain processing
          no                Negative or set default values of a command
          public-key        DNSCrypt provider public key
          registration-vrf  Cloud facing vrf
          resolver          Anycast address
          token             Config umbrella token
          udp-timeout       Config timeout value for UDP sessions
          vrf               Configure VRF

Per-VRF options are provided under VRF option:
Device(config)# parameter-map type umbrella global
Device(config-profile)#vrf 9
Device(config-profile-vrf)#?
vrf options:
    dns-resolver        DNS resolver address
    exit                Exit from vrf sub mode
    match-local-domain  Match local-domain list(if configured)
    no                  Negate a command or set its defaults

 parameter-map type regex dns_bypass
 pattern www.cisco.com
 pattern .*amazon.com
 pattern .*.salesforce.com
!
parameter-map type umbrella global
token 648BF6139C379DCCFFBA637FD1E22755001CE241
local-domain dns_bypass
dnscrypt udp-timeout 5
vrf 9
      dns-resolver 8.8.8.8
      match-local-domain
vrf 19
      dns-resolver 8.8.8.8
      no match-local-domain
 vrf 29
      dns-resolver umbrella
      match-local-domain
 vrf 39
      dns-resolver umbrella
      no match-local-domain
!
```

The following table captures the per VRF DNS packet behavior:

VRF	dns-resolver	Match-local-domain (dns_bypass)
9	8.8.8.8	Yes
19	8.8.8.8	No
29	umbrella	Yes
39	umbrella	No

Note The VRFs must be preconfigured. For example, the VRFs 9,19, 29, 39 are preconfigured in the above example.

Sample NAT config for DIA internet connectivity:

```
ip access-list extended dia-nat-acl
10 permit ip any any
ip nat inside source list dia-nat-acl interface <WAN-facing-Interface> overload
“ip nat outside” MUST be configured under <WAN-facing-Interface>
```

Configure the Device as a Pass-through Server

You can identify the traffic to be bypassed using domain names. In the SD-WAN 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 Umbrella cloud. This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

```
Device# config-transaction
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.cisco.com
Device(config)# pattern .*amazon.com
Device(config)# pattern .*.salesforce.com
```

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
- Public-Key

Public-key

Public-key is used to download the DNSCrypt certificate from 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 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 device and the Umbrella Integration. When the **parameter-map type umbrella** is configured and enabled by default on all WAN interfaces. 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.

Sample umbrella dnscrypt notifications:

```
Device# show sdwan 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 Successfull Attempt: 08:46:32 IST May 21 2018
  Certificate Details:
```

```
           Certificate Magic     : DNSC
           Major Version         : 0x0001
           Minor Version         : 0x0000
           Query Magic           : 0x714E7A696D657555
           Serial Number         : 1517943461
           Start  Time           : 1517943461 (00:27:41 IST Feb 7 2018)
           End Time              : 1549479461 (00:27:41 IST Feb 7 2019)
         Server Public Key    : 240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836

         Client Secret Key Hash: 8A97:BBD0:A8BE:0263:F07B:72CB:BB21:330B:D47C:7373:B8C8:5F96:9F07:FEC6:BBFE:95D0

         Client Public key    : 0622:C8B4:4C46:2F95:D917:85D4:CB91:5BCE:78C0:F623:AFE5:38BC:EF08:8B6C:BB40:E844

         NM key Hash          : 88FC:7825:5B58:B767:32B5:B36F:A454:775C:711E:B58D:EE6C:1E5A:3BCA:F371:4285:5E3A
When disabled:
Device# show umbrella dnscrypt
       DNSCrypt: Not enabled
       Public-key: NONE

Sample configuration steps for dns-resolver and match-local-domain-to-bypass per vrf:
Router(config)# vrf definition 1
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commitCommit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# ?
Possible completions:
    dnscrypt
    local-domain
    public-key
    registration-vrf
    resolver
    token
    udp-timeout
    vrf
Router(config-profile)# vrf ?
This line doesn't have a valid range expression
Possible completions:
    <name:string, min: 1 chars, max: 32 chars>  1
Router(config-profile)# vrf 1
Router(config-profile-vrf)# ?
Possible completions:
    dns-resolver
    match-local-domain-to-bypass
Router(config-profile-vrf)# dns-resolver umbrella
Router(config-profile-vrf)# match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router(config)# vrf definition 2
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commitCommit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# vrf 2
Router(config-profile-vrf)# dns-resolver 8.8.8.8
Router(config-profile-vrf)# no match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router#sh 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
Registration VRF: default
VRF List:
1. VRF 1 (ID: 1)
    DNS-Resolver: umbrella
    Match local-domain-to-bypass: Yes
2. VRF 2 (ID: 3)
    DNS-Resolver: 8.8.8.8
    Match local-domain-to-bypass: No
```

Verify the Umbrella Connector Configuration

Verify the Umbrella Connector configuration using the following commands:

```
Device# show umbrella config
Umbrella Configuration
========================
  Token: 648BF6139C379DCCFFBA637FD1E22755001CE241
  OrganizationID: 1892929
  Local Domain Regex parameter-map name: dns_bypass
  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
  Registration VRF: default
  VRF List:
      1. VRF 9 (ID: 4)
          DNS-Resolver: 8.8.8.8
          Match local-domain: Yes
      2. VRF 19 (ID: 1)
          DNS-Resolver: 8.8.8.8
          Match local-domain: No
      3. VRF 29 (ID: 2)
          DNS-Resolver: umbrella
          Match local-domain: Yes
      4. VRF 39 (ID: 3)
          DNS-Resolver: umbrella
          Match local-domain: No
The output of VRF will have name and ID. The ID here is VRF ID:
Device# show vrf detail | inc VRF Id
VRF 19 (VRF Id = 1); default RD <not set>; default VPNID <not set>
VRF 29 (VRF Id = 2); default RD <not set>; default VPNID <not set>
VRF 39 (VRF Id = 3); default RD <not set>; default VPNID <not set>
VRF 9 (VRF Id = 4); default RD <not set>; default VPNID <not set>

When DNSCrypt is disabled:
Device# show umbrella config
Umbrella Configuration
```

```
========================
    Token: 648BF6139C379DCCFFBA637FD1E22755001CE241
    OrganizationID: 1892929
    Local Domain Regex parameter-map name: dns_bypass
    DNSCrypt: Not enabled
    Public-key: NONE
    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
 Registration VRF: default
 VRF List:
     1. VRF 9 (ID: 4)
         DNS-Resolver: 8.8.8.8
         Match local-domain: Yes
     2. VRF 19 (ID: 1)
         DNS-Resolver: 8.8.8.8
         Match local-domain: No
     3. VRF 29 (ID: 2)
         DNS-Resolver: umbrella
         Match local-domain: Yes
    4. VRF 39 (ID: 3)
        DNS-Resolver: umbrella
        Match local-domain: No
```

Display Umbrella Registration Details

The following example displays the device registration information:

```
Device# show sdwan umbrella device-registration
Device registration details
VRF        Tag     Status          Device-id29
vpn29      200     SUCCESS     010a9b2b0d5cb21f39
vpn39      200     SUCCESS     010a1a2e1989da19

The following example displays the device registration information in detail:
Device# show umbrella deviceid detailed
Device registration details
1.29
    Tag               : vpn29
    Device-id         : 010a9b2b0d5cb21f
    Description       : Device Id recieved successfully
    WAN interface     : None

2.39
    Tag               : vpn39
    Device-id         : 010a1a2e1989da19
    Description       : De
    vice Id recieved successfully
    WAN interface     : None
```

Configure Cisco Umbrella Using a CLI Device Template

For more information on using the CLI device template, see Device Configuration-Based CLI Templates for Cisco IOS XE SD-WAN Devices.

This section provides example CLI configurations for Cisco Umbrella.

```
secure-internet-gateway
umbrella org-id <umbrella org id>
umbrella api-key <api key>
umbrella api-secret "<secret key>"
```

```
sdwan
interface Tunnel100001
  tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc
 source-interface GigabitEthernet0/0/0
  exit
  interface Tunnel100002
  tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference secondary-dc
 source-interface GigabitEthernet0/0/0
  exit

service sig vrf global
  ha-pairs
   interface-pair Tunnel100001 active-interface-weight 1 Tunnel100002 backup-interface-weight1


vrf definition <vrf#>
address-family ipv4
exit-address-family

interface Loopback<some value>
no shutdown
  vrf forwarding <vrf#>
ip address <IP Address> <mask>
exit

interface Tunnel100001
 no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip clear-dont-fragment
  ip tcp adjust-mss 1300
  ip mtu 1400
  tunnel source GigabitEthernet<#/#/#>
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec1-ipsec-profile
  tunnel vrf multiplexing
  tunnel route-via GigabitEthernet<###> mandatory
exit
interface Tunnel100002
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip clear-dont-fragment
  ip tcp adjust-mss 1300
  ip mtu 1400
  tunnel source GigabitEthernet<#/#/#>
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec2-ipsec-profile
  tunnel vrf multiplexing
  tunnel route-via GigabitEthernet<###> mandatory
exit

crypto ikev2 policy policy1-global
  proposal p1-global

crypto ikev2 profile if-ipsec1-ikev2-profile
  no config-exchange request
  dpd 10 3 on-demand
  dynamic
  lifetime 86400

crypto ikev2 profile if-ipsec2-ikev2-profile
  no config-exchange request
 dpd 10 3 on-demand
  dynamic
  lifetime 86400

crypto ikev2 proposal p1-global
  encryption aes-cbc-128 aes-cbc-256
  group 14 15 16
  integrity sha1 sha256 sha384 sha512

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256

crypto ipsec transform-set if-ipsec2-ikev2-transform esp-gcm 256

crypto ipsec profile if-ipsec1-ipsec-profile
  set ikev2-profile if-ipsec1-ikev2-profile
  set transform-set if-ipsec1-ikev2-transform
  set security-association lifetime kilobytes disable
  set security-association lifetime seconds 3600
  set security-association replay window-size 512

crypto ipsec profile if-ipsec2-ipsec-profile
  set ikev2-profile if-ipsec2-ikev2-profile
  set transform-set if-ipsec2-ikev2-transform
  set security-association lifetime kilobytes disable
  set security-association lifetime seconds 3600
  set security-association replay window-size 512
```

Umbrella show commands at FP Layer

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

```
Device# show platform software umbrella f0 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
2620:119:35::35
2620:119:53::53
Dnscrypt Info:
public_key:
A5:BA:18:C5:59:70:67:94:E5:37:38:33:06:F9:63:83:39:86:82:E4:00:F5:D8:BE:C1:AA:77:4A:4C:BA:64:00
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461
ProfileID    DeviceID          Mode      Resolver     Local-Domain    Tag
------------------------------------------------------------------------------
     0                         OUT                      False
     4                         IN        8.8.8.8        True           vpn9
     1                         IN        8.8.8.8        False          vpn19
     2     010a9b2b0d5cb21f    IN     208.67.220.220    True           vpn29
     3     010a1a2e1989da19    IN     208.67.220.220    False          vpn39

The show platform software umbrella f0 local-domain displays the local domain list.
Device# show platform software umbrella f0 local-domain
01.  www.cisco.com
02.  www.amazon.com
03.  .*sales.abc.*
```

Umbrella show commands at CPP Layer

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

```
 +++ 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:
D9:2D:20:93:E8:8C:B4:BD:32:E6:A3:D1:E0:5B:7E:1A:49:C5:7F:96:BD:28:79:06:A2:DD:2E:A7:A1:F9:3D:7E
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461

Umbrella Interface Config:
--------------------------
11      GigabitEthernet4 :
        Mode     : IN
        DeviceID : 010a9b2b0d5cb21f
        Tag      : vpn29
10      GigabitEthernet3 :
        Mode     : IN
        DeviceID : 0000000000000000
        Tag      : vpn9
05      Null0 :
        Mode     : OUT
06     VirtualPortGroup0 :
        Mode     : OUT
07     VirtualPortGroup1 :
        Mode     : OUT
08      GigabitEthernet1 :
        Mode     : OUT
09      GigabitEthernet2 :
        Mode     : OUT
12      GigabitEthernet5 :
        Mode     : OUT

Umbrella Profile Deviceid Config:
----------------------------------
```

```
ProfileID: 0
    Mode     : OUT
ProfileID: 1
    Mode     : IN
    Resolver : 8.8.8.8
    Local-Domain: False
    DeviceID : 0000000000000000
    Tag      : vpn19
ProfileID: 3
    Mode     : IN
    Resolver : 208.67.220.220
    Local-Domain: False
    DeviceID : 010a1a2e1989da19
    Tag      : vpn39
ProfileID: 4
    Mode     : IN
    Resolver : 8.8.8.8
    Local-Domain: True
    DeviceID : 0000000000000000
    Tag      : vpn9
ProfileID: 2
    Mode     : IN
    Resolver : 208.67.220.220
    Local-Domain: True
    DeviceID : 010a9b2b0d5cb21f
    Tag      : vpn29

Umbrella Profile ID CPP Hash:
------------------------------
VRF ID :: 1
    VRF NAME : 19
    Resolver : 8.8.8.8
    Local-Domain: False
VRF ID :: 4
    VRF NAME : 9
    Resolver : 8.8.8.8
    Local-Domain: True
VRF ID :: 2
    VRF NAME : 29
    Resolver : 208.67.220.220
    Local-Domain: True
VRF ID :: 3
    VRF NAME : 39
    Resolver : 208.67.220.220
    Local-Domain: False
```

Umbrella Data-Plane show commands

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

```
Device# show platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats:
    Parser statistics:
        parser unknown pkt: 0
        parser fmt error: 0
        parser count nonzero: 0
        parser pa error: 0
        parser non query: 0
        parser multiple name: 0
        parser dns name err: 0
        parser matched ip: 0
        parser opendns redirect: 0
        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 : 0
        feature object frees  : 0
        flow create requests  : 0
        flow create successful: 0
        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  : 0
        flow lookup successful: 0
        flow lookup failed, CFT handle: 0
        flow lookup failed, getting FO: 0
        flow lookup failed, no match  : 0
        flow detach requests  : 0
        flow detach successful: 0
        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: 0
         clear sent: 0
         enc sent: 0
         clear rcvd: 0
         dec rcvd: 0
         pa err: 0
         enc lib err: 0
         padding err: 0
         nonce err: 0
         flow bypass: 0
         disabled: 0
         flow not enc: 0
    DCA statistics:
        dca match success: 0
        dca match failure: 0
```

The **show platform hardware qfp active feature umbrella datapath memory** command displays CFT information.

```
Device# show platform hardware qfp active feature umbrella datapath memory
==Umbrella Connector CFT Information==
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
==Umbrella Connector Runtime Information==
umbrella init state 0x4
umbrella dsa client handler 0x2
```

The **show platform hardware qfp active feature umbrella datapath runtime** command displays internal information. For example, key index used for DNSCrypt.

```
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: 1517943461
ref cnt: 0
magic: 714e7a696d657555
Client Public Key:
A5BA:18C5:5970:6794:E537:3833:06F9:6383:3986:82E4:00F5:D8BE:C1AA:774A:4CBA:6400
NM Key Hash      :
16E6:DDC7:53BE:2929:1CDA:06AE:0BE2:C270:6E39:EAE7:F925:78FD:3599:2AB6:74C9:A59D
-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
Local domain 1
VPN-DEVICEID TABLE d7f37410
```

Clear Command

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 the Umbrella Integration

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

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

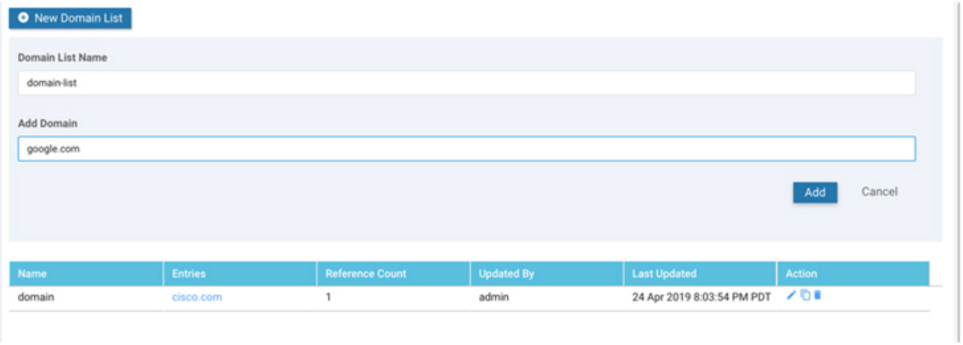
Depending on the OS, run either of these two commands from the client device:

- 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)"
```

DNS Security Policy Configuration

Domain List



Domain List Name: domain-list

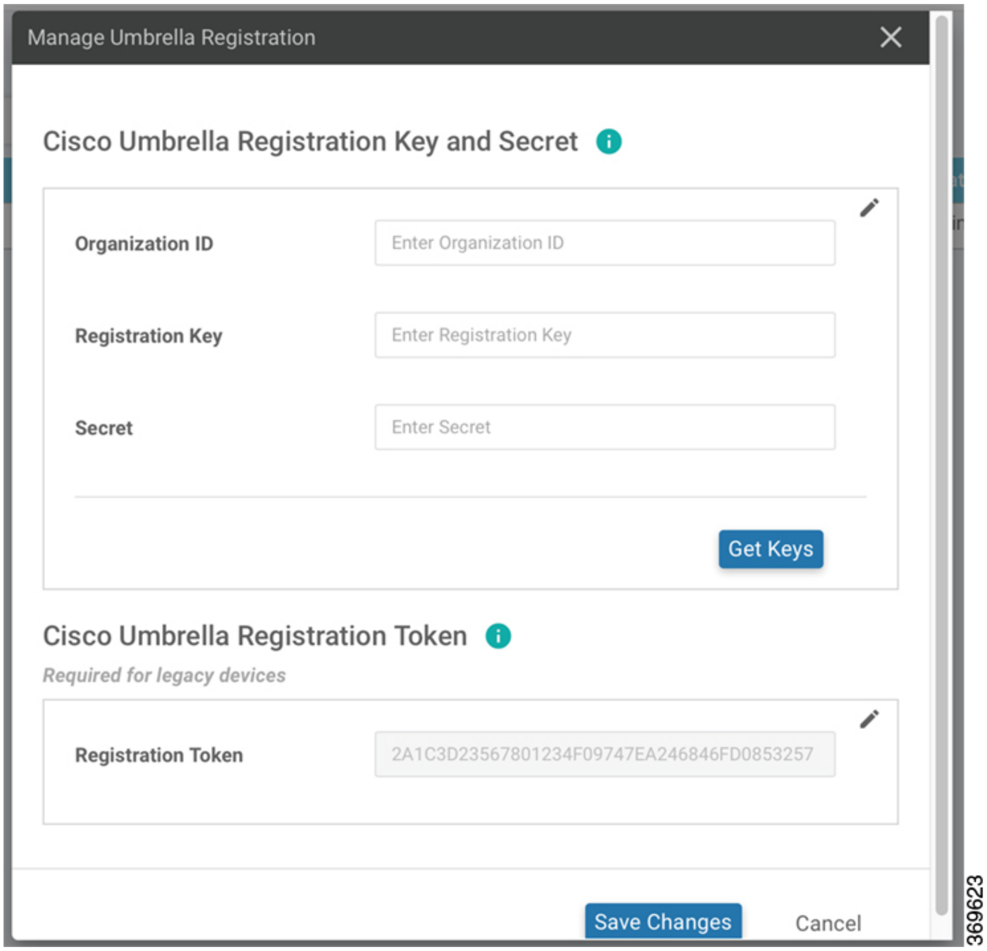
Add Domain: google.com

Name	Entries	Reference Count	Updated By	Last Updated	Action
domain	cisco.com	1	admin	24 Apr 2019 8:03:54 PM PDT	

369619

CLI Command	Possible Completions	Description and possible input values
policy lists local-domain-list <name>		List of domain name regular expression patterns
		Domain name regular expression pattern string. For example, policy lists local-domain-list name as google.com.

Umbrella Registration


Manage Umbrella Registration

Cisco Umbrella Registration Key and Secret

Organization ID: Enter Organization ID

Registration Key: Enter Registration Key

Secret: Enter Secret

Cisco Umbrella Registration Token

Required for legacy devices

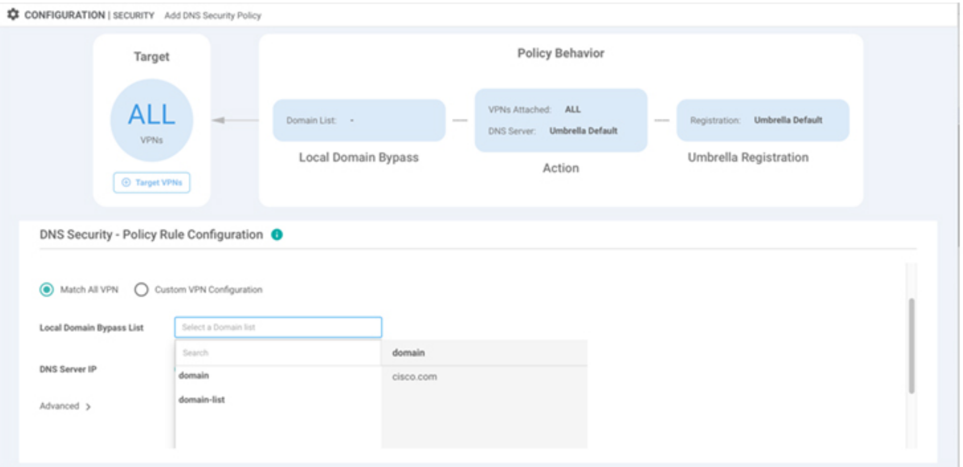
Registration Token: 2A1C3D23567801234F09747EA246846FD0853257

CLI Command	Possible Completions	Description and possible input values
security umbrella		Configure Umbrella service related security properties.
	api-key	Config umbrella api-key. The value ranges from 1 to 64 characters.
	dnscrypt	Enable DNScrypt while redirecting DNS requests to Umbrella.
	orgid	Config umbrella org id
	secret	Config umbrella secret. The value can be [0 | 6].
	token	Umbrella service registration token. The value ranges from 1 to 64 characters.

CLI Command	Possible Completions	Description and possible input values
vpn <number, range>	**dns-redirect match-local-domain-to-bypass**	List of domain name regular expression patterns

	dns-redirect umbrella	Bypass the dns redirect for entries in the local domain list Use Umbrella as DNS redirect service.

DNS-Security Policy with Domain List



CONFIGURATION | SECURITY Add DNS Security Policy

Target

ALL VPNs

⊕ Target VPNs

Policy Behavior

Domain List: -

Local Domain Bypass

VPNs Attached: ALL

DNS Server: Umbrella Default

Action

Registration: Umbrella Default

Umbrella Registration

DNS Security - Policy Rule Configuration

● Match All VPN ○ Custom VPN Configuration

Local Domain Bypass List: Select a Domain list

Search	domain
domain	cisco.com
domain-list	

DNS Server IP

Advanced >

369618

```
policy
 lists
  local-domain-list domain-list
    google.com
  !
  exit
 !
!
exit
!
security
 umbrella
  dnscrypt
!
exit
!
vpn matchAllVpn
 dns-redirect umbrella match-local-domain-to-bypass
```