

DNS Policies for Security Intelligence

The following topics explain DNS policies, DNS rules, and how to deploy DNS policies to managed devices.

- DNS policies, on page 1
- Cisco umbrella DNS policies, on page 2
- DNS policy components, on page 3
- License requirements for DNS policies, on page 4
- Requirements and prerequisites for DNS policies, on page 4
- Managing DNS and Umbrella DNS Policies, on page 4
- DNS rules, on page 6
- DNS rules, on page 13
- Requirement: deploy DNS policy configuration changes, on page 19
- Cisco umbrella DNS policies, on page 19
- DNS over HTTPs and QUIC, on page 25

DNS policies

A DNS policy is a security configuration that

- blocks traffic based on the domain name requested by a client, using a Security Intelligence Block list
- uses Cisco-provided domain name intelligence to filter traffic
- supports custom lists and feeds of domain names tailored to your deployment, and
- requires association with an access control policy for deployment to managed devices.

DNS policy behavior

Traffic on a DNS policy Block list is immediately blocked and therefore is not subject to any further inspection—not for intrusions, exploits, malware, and so on, but also not for network discovery. You can use a Security Intelligence Do Not Block list to override a Block list and force access control rule evaluation, and, recommended in passive deployments, you can use a "monitor-only" setting for Security Intelligence filtering. This allows the system to analyze connections that would have been blocked by a Block list, but also logs the match to the Block list and generates an end-of-connection Security Intelligence event.

Note DNS-based Security Intelligence may not work as intended for a domain name unless the DNS server deletes a domain cache entry due to expiration, or a client's DNS cache or the local DNS server's cache is cleared or expires.

You configure DNS-based Security Intelligence using a DNS policy and associated DNS rules. To deploy it to your devices, you must associate your DNS policy with an access control policy, then deploy your configuration to managed devices.

Cisco umbrella DNS policies

A Cisco Umbrella DNS policy is a security mechanism that

- redirects DNS queries to Cisco Umbrella for domain validation and policy enforcement,
- allows or blocks requests based on domain names and applies DNS-based security policies, and
- provides two lines of protection through local DNS inspection and cloud-based Cisco Umbrella policies.

DNS query redirection process

Cisco Umbrella DNS Connection in the management center helps to redirect DNS queries to Cisco Umbrella. This allows Cisco Umbrella to validate requests, allow or block them based on the domain names, and apply DNS-based security policy on the request. If you use Cisco Umbrella, you must configure the Cisco Umbrella Connection (**Integrations** > **Cloud Services** and choose the **Cisco Umbrella Connection**) to redirect DNS queries to Cisco Umbrella.

The Umbrella Connector is part of the system's DNS inspection. If your existing DNS inspection policy map decides to block or drop a request based on your DNS inspection settings, the request is not forwarded to Cisco Umbrella. Thus, you have two lines of protection:

- Your local DNS inspection policy
- Your Cisco Umbrella cloud-based policy

When redirecting DNS lookup requests to Cisco Umbrella, the Umbrella Connector adds an EDNS (Extension mechanisms for DNS) record. An EDNS record includes the device identifier information, organization ID, and client IP address. Your cloud-based policy can use those criteria to control access in addition to the reputation of the FQDN. You can also elect to encrypt the DNS request using DNSCrypt to ensure the privacy of usernames and internal IP addresses.

To redirect DNS requests from the management center to Cisco Umbrella:

1. Configure the Cisco Umbrella connection settings.
2. Create and configure an Umbrella DNS policy.
3. Associate the Umbrella DNS policy with an access control policy.
4. Deploy the changes.

For detailed information about how to set up the Umbrella DNS Connector in the management center, see Configuring the Umbrella DNS Connector for Cisco Secure Firewall Management Center.

DNS policy components

DNS policy components are configuration elements that

- enable blocking of connections based on domain name using a Block list
- exempt connections from blocking using a Do Not Block list, and
- provide granular network traffic handling through configurable rules and settings.

DNS policy configuration options

These configurations can be changed after creating a DNS policy:

- **Name and Description**: Each DNS policy must have a unique name. A description is optional.
- **Rules**: Rules provide a granular method of handling network traffic based on the domain name. Rules in a DNS policy are numbered, starting at 1. The system matches traffic to DNS rules in top-down order by ascending rule number.

When you create a DNS policy, the system populates it with a default Global Do-Not-Block List for DNS rule and a default Global Block List for DNS rule. Both rules are fixed to the first position in their respective categories. You cannot modify these rules, but you can disable them.



Note If multitenancy is enabled for your Cloud-Delivered Firewall Management Center, the system is organized into a hierarchy of domains, including ancestor and descendant domains. These domains are distinct and separate from the domain names used in DNS management.

A descendant list contains the domains on the Block or Do Not Block lists of system subdomain users. From an ancestor domain, you cannot view the contents of descendant lists. If you do not want subdomain users to add domains to a Block or Do Not Block list:

- disable the descendant list rules, and
- enforce Security Intelligence using the access control policy inheritance settings

The system evaluates rules in this order:

1. Global Do-Not-Block List for DNS rule (if enabled)
2. Descendant DNS Do-Not-Block Lists rule (if enabled)
3. Rules with a Do Not Block action
4. Global Block List for DNS rule (if enabled)
5. Descendant DNS Block Lists rule (if enabled)
6. Rules with an action other than Do Not Block

Usually, the system handles DN-based network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic. If no DNS rules match the traffic, the system continues evaluating the traffic based on the associated access control policy's rules. DNS rule conditions can be simple or complex.

License requirements for DNS policies

This reference provides the license requirements necessary for implementing DNS policies across different Firepower system configurations.

Threat Defense License

IPS

Classic License

Protection

Requirements and prerequisites for DNS policies

This reference provides the requirements and prerequisites needed to configure and implement DNS policies, including model support, domain compatibility, and required user roles.

Model support

Any

Supported domains

Any

User roles

- Administrator
- Access Admin
- Network Admin



Important You must apply the Network Discovery policy on the device for a successful DNS validation on the traffic.

Managing DNS and Umbrella DNS Policies

Use the DNS Policy page to create, edit, delete, copy, and compare custom DNS and Umbrella DNS policies for comprehensive network security management.

Use the DNS Policy page (**Policies** > **Security policies** > **DNS**) to manage custom DNS and Umbrella DNS policies.

In addition to custom policies that you create, the system provides the Default DNS Policy and Default Umbrella DNS Policy. The default DNS policy uses the default Block list and Do Not Block list. You can edit and use this system-provided custom policies.

Procedure

Step 1 Choose **Policies** > **Security policies** > **DNS**.

Step 2 Manage your DNS policy:

- Compare—To compare DNS policies, click **Compare Policies** and proceed as described in Compare policies.
- Copy—To copy a DNS policy, click **Copy** ( ) and proceed as described in Edit DNS policies, on page 6.
- Create—To create a new Umbrella DNS policy, click **New Policy** > **Umbrella DNS Policy** and proceed as described in Create an umbrella DNS policy, on page 22.
- Delete—To delete a DNS or Umbrella DNS policy, click **Delete** ( ), then confirm you want to delete the policy.
- Edit—To modify an existing DNS policy, click **Edit** ( )) and proceed as described in Edit DNS policies, on page 6. To modify an existing Umbrella DNS policy, click **Edit** ( )) and proceed as described in Edit Umbrella DNS policies and rules, on page 23.

You have successfully managed your DNS policies. The policies are now available for deployment to your network devices for DNS-based security filtering.

Create basic DNS policies

Creating a basic DNS policy establishes a foundation for DNS traffic filtering and management that you can customize to meet your organization's security requirements.

When you create a new DNS policy, it contains default settings. You must then edit it to customize the behavior.

Follow these steps to create a basic DNS policy:

Procedure

Step 1 Choose **Policies** > **Security policies** > **DNS**.

Step 2 Click **Add DNS Policy** > **DNS Policy**.

Step 3 Give the policy a unique **Name** and, optionally, a **Description**.

Step 4 Click **Save**.

The DNS policy is created with default settings and appears in the DNS policies list.

What to do next

Configure the policy. See Edit DNS policies, on page 6.

Edit DNS policies

Edit DNS policies to update policy configurations, modify rule settings, and maintain network security requirements.

Only one person should edit a DNS policy at a time, using a single browser window. If multiple users attempt to save the same policy, only the first set of saved changes are retained.

To protect the privacy of your session, after thirty minutes of inactivity on the policy editor, a warning appears. After sixty minutes, the system discards your changes.

Procedure

Step 1 Choose **Policies** > **Security policies** > **DNS**.

Step 2 Click **Edit** (✎) next to the DNS policy you want to edit.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Edit your DNS policy:

- Name and Description—To change the name or description, click the field and type the new information.
- Rules—To add, categorize, enable, disable, or otherwise manage DNS rules, click **Rules** and proceed as described in Create and edit DNS rules, on page 7.

Step 4 Click **Save**.

The DNS policy is updated with your changes and ready for deployment.

What to do next

- Optionally, further configure the new policy as described in *Logging Connections with Security Intelligence* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Deploy configuration changes; see Deploy configuration changes.

DNS rules

A DNS rule is a Security Intelligence component that

- handles traffic based on the domain name requested by a host,
- operates after any traffic decryption and before access control evaluation, and
- matches traffic in the order specified, with the system handling network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic.

DNS rule components

In addition to its unique name, each DNS rule has these basic components:

- **State**: By default, rules are enabled. If you disable a rule, the system does not use it to evaluate network traffic, and stops generating warnings and errors for that rule.
- **Position**: Rules in a DNS policy are numbered, starting at 1. The system matches traffic to rules in top-down order by ascending rule number. With the exception of Monitor rules, the first rule that traffic matches is the rule that handles that traffic.
- **Conditions**: Conditions specify the specific traffic the rule handles. A DNS rule must contain a DNS feed or list condition, and can also match traffic by security zone, network, dynamic attributes, or VLAN.
- **Action**: A rule's action determines how the system handles matching traffic.

A rule's action determines how the system handles matching traffic:

- Traffic with a **Do Not Block** action is allowed, subject to further access control inspection.
- Monitored traffic is subject to further evaluation by remaining rules on the DNS Block list. If the traffic does not match a DNS Block list rule, it is inspected with access control rules. The system logs a Security Intelligence event for the traffic.
- Traffic on a Block list is dropped without further inspection. You can also return a Domain Not Found response, or redirect the DNS query to a sinkhole server.

Related Topics

Security intelligence

Create and edit DNS rules

Create and edit DNS rules to define how the system handles DNS queries by specifying actions and conditions for domain name resolution.

In a DNS policy, you can add up to a total of 32767 DNS lists to the Block list and Do Not Block list rules; that is, the number of lists in the DNS policy cannot exceed 32767.

Follow these steps to create and edit DNS rules:

Procedure

Step 1 In the DNS policy editor, you have the following options:

- To add a new rule, click **Add DNS Rule**.
- To edit an existing rule, click **Edit** ( ).

Step 2 Enter a **Name**.

Step 3 Configure the rule components, or accept the defaults:

- Action—Choose a rule **Action**; see DNS rule actions, on page 9.
- Conditions—Configure the rule's conditions; see DNS rule conditions, on page 10.
- Enabled—Specify whether the rule is **Enabled**.

Step 4 Click **Save**.

The DNS rule is created or updated with the specified configuration and is ready for deployment.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

DNS rule management

DNS rule management is a policy administration feature that enables you to add, edit, move, enable, disable, delete, and otherwise manage DNS rules within your policy.

DNS rule management interface

The **Rules** tab of the DNS policy editor provides the interface for DNS rule management operations.

For each rule, the policy editor displays this information:

- Rule name
- Summary of rule conditions
- Rule action

Additional icons represent **Warning** (), **Error** (), and other important **Information** (). Disabled rules are dimmed and marked `(disabled)` beneath the rule name.

Enable and disable DNS rules

Enable or disable DNS rules to control whether the system uses them to evaluate network traffic and generate warnings and errors.

When you create a DNS rule, it is enabled by default. If you disable a rule, the system does not use it to evaluate network traffic and stops generating warnings and errors for that rule. When viewing the list of rules in a DNS policy, disabled rules are dimmed, although you can still modify them. Note that you can also enable or disable a DNS rule using the DNS rule editor.

Follow these steps to enable or disable DNS rules:

Procedure

Step 1 In the DNS policy editor, right-click the rule and choose a rule state.

Step 2 Click **Save**.

The DNS rule state is updated. Disabled rules appear dimmed in the policy rule list but can still be modified.

What to do next

- Deploy configuration changes.

DNS rule order evaluation

DNS rule order evaluation is a traffic processing mechanism that

- matches traffic to DNS rules in top-down order by ascending rule number,
- handles network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic, and
- applies different continuation behavior based on rule type.

Rule evaluation behavior

Rules in a DNS policy are numbered, starting at 1. The system behavior differs based on rule type:

- For Monitor rules, the system logs the traffic, then continues evaluating traffic against lower-priority DNS Block list rules.
- For non-Monitor rules, the system does **not** continue to evaluate traffic against additional, lower-priority DNS rules after that traffic matches a rule.

Rule order precedence follows this hierarchy:

- The Global Do-Not-Block List for DNS is always first, and takes precedence over all other rules.
- The Do-Not-Block List section precedes the Block List section; Do-Not-Block List rules always take precedence over other rules.
- The Global Block List for DNS is always first in the Block List section, and takes precedence over all other Monitor and Block list rules.
- The Block List section contains Monitor and Block list rules.
- When you first create a DNS rule, the system positions it last in the Do-Not-Block List section if you assign a **Do Not Block** action, or last in the Block List section if you assign any other action.

You can drag and drop rules to reorder them.

DNS rule actions

A DNS rule action is a configuration setting that

- determines handling for matching traffic, governing whether the system will block, not block, or monitor traffic based on rule conditions,
- controls logging behavior, determining when and how details about matching traffic are recorded, and
- impacts action prioritization when configured with TID.

DNS rule action types

DNS rules support these action types:

- **Do Not Block**: Allows traffic to pass to the next phase of inspection, which is access control rules. The system does not log *Do Not Block list* matches. Logging of these connections depends on their eventual disposition.
- **Monitor**: Forces connection logging; matching traffic is neither immediately allowed nor blocked. Traffic is matched against additional rules to determine whether to permit or deny it. The first non-Monitor DNS rule matched determines whether the system blocks the traffic. If there are no additional matching rules, the traffic is subject to access control evaluation. For connections monitored by a DNS policy, the system logs end-of-connection Security Intelligence and connection events to the Cloud-Delivered Firewall Management Center database.
- **Drop**: Drops the traffic without further inspection.
- **Domain Not Found**: Returns a non-existent internet domain response to the DNS query, which prevents the client from resolving the DNS request.
- **Sinkhole**: Returns a sinkhole object's IPv4 or IPv6 address in response to the DNS query (A and AAAA records only). The sinkhole server can log, or log and block, follow-on connections to the IP address. If you configure a **Sinkhole** action, you must also configure a sinkhole object.

Logging behavior varies based on the action type:

- For a connection blocked based on the **Drop** or **Domain Not Found** actions, the system logs beginning-of-connection Security Intelligence and connection events. Because blocked traffic is immediately denied without further inspection, there is no unique end of connection to log.
- For a connection blocked based on the **Sinkhole** action, logging depends on the sinkhole object configuration. If you configure your sinkhole object to only log sinkhole connections, the system logs end-of-connection connection events for the follow-on connection. If you configure your sinkhole object to log and block sinkhole connections, the system logs beginning-of-connection connection events for the follow-on connection, then blocks that connection.

DNS rule conditions

A DNS rule condition is a traffic identification criterion that

- identifies the type of traffic that rule handles,
- can be simple or complex, and
- must include a DNS feed or list condition within a DNS rule.

DNS rule condition requirements

You can also optionally control traffic by security zone, network, dynamic attributes, or VLAN.

When adding conditions to a DNS rule:

- If you do not configure a particular condition for a rule, the system does not match traffic based on that criterion.

- You can configure multiple conditions per rule. Traffic must match **all** the conditions in the rule for the rule to apply to traffic. For example, a rule with a DNS feed or list condition and network condition but no VLAN tag condition evaluates traffic based on the domain name and source or destination, regardless of any VLAN tagging in the session.
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches **any** of a condition's criteria satisfies the condition. For example, you can use a single rule to block traffic based on up to 50 DNS lists and feeds.

Security zone rule conditions

A security zone rule condition is a network traffic control mechanism that

- segments your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices,
- controls or decrypts traffic by its source and destination security zones, and
- requires all interfaces in a zone to be of the same type (all inline, passive, switched, or routed).

Zone condition traffic matching

If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

All zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Tip Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of device's interfaces, that rule does not affect that device's performance.

Network rule conditions

A network condition is a traffic matching criterion that

- matches traffic for rate limiting based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Note You *cannot* use FQDN network objects in identity rules.

VLAN tag rule conditions

VLAN tags rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

VLAN tag rule conditions configuration details

Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

DNS policy rule conditions

A DNS policy rule condition is a DNS rule component that

- allows you to control traffic if a DNS list, feed, or category contains the domain name requested by the client,
- must be defined in a DNS rule, and
- applies the configured rule action to traffic regardless of whether you add a global or custom Block or Do Not Block list.

DNS condition behavior

The system applies the configured rule action to the traffic regardless of the list type. For example, if you add the Global Do Not Block List to a rule, and configure a **Drop** action, the system blocks all traffic that should have been allowed to pass to the next phase of inspection.

Dynamic attributes rule conditions

A dynamic attributes rule condition is a DNS rule matching mechanism that

- uses dynamic objects containing IP addresses or endpoint device type objects for source or destination matching,
- uses Security Group Tag (SGT) objects containing manually defined tags or ISE-defined tags for source-only matching, and
- applies logical operations where objects of the same type are ORed together and objects of different types are ANDed together.

Dynamic attributes configuration and behavior

You can use these types of dynamic attributes to match connections in DNS rules:

- (Source or destination.) Dynamic objects, which contain IP addresses. Endpoint device type objects are source only. For more information, see Dynamic objects and the chapter on Dynamic Attributes Connector.
- (Source only.) Security Group Tag (SGT) objects, which contain tags either manually defined or defined through ISE. For more information, see Source and destination security group tag (SGT) matching and Security group tags.

When you configure dynamic attributes for a DNS rule, objects of the same type in the same source or destination list are ORed together and objects of different types are ANDed together. For example, if you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originates from (or is destined to) one of those IP addresses.

Initially, all **Dynamic Objects** and **Security Group Tags** are listed when you open the **Dynamic Attributes** tab. You can deselect an option to remove those objects from the list. You can also start typing in the search box to find the object you want.

DNS rules

A DNS rule is a network security mechanism that controls and filters DNS queries and responses within network traffic

Control traffic based on DNS and security zone

Control traffic flow by implementing DNS rules with security zone conditions to manage network access and security policies.

Zone conditions in DNS rules allow you to control traffic by its source security zone. A *security zone* is a grouping of one or more interfaces, which may be located across multiple devices.

Procedure

Step 1 In the DNS rule editor, click **Zones**.

Step 2 Find and select the zones you want to add from the **Available Zones**. To search for zones to add, click the **Search by name** prompt above the **Available Zones** list, then type a zone name. The list updates as you type to display matching zones.

Step 3 Click to select a zone, or right-click and then select **Select All**.

Step 4 Click **Add to Source**, or drag and drop.

Step 5 Click the **DNS** tab and add the lists or feeds that include the DNS names you are controlling. For more information, see Control traffic based on DNS list or feed, on page 16.

Step 6 Save or continue editing the rule.

The DNS rule is configured with security zone conditions to control traffic based on source security zones and DNS names.

What to do next

- Deploy configuration changes.

Control traffic based on DNS and network

Control traffic by explicitly specifying the source IP addresses for the traffic you want to manage through DNS rules.

Network conditions in DNS rules allow you to control traffic by its source IP address. You can explicitly specify the source IP addresses for the traffic you want to control.

Procedure

Step 1 In the DNS rule editor, click **Networks**.

Step 2 Find and select the networks you want to add from the **Available Networks**, as follows:

- To add a network object on the fly, which you can then add to the condition, click **Add** (+) above the **Available Networks** list and proceed as described in Create a network object.
- To search for network objects to add, click the **Search by name or value** prompt above the **Available Networks** list, then type an object name or the value of one of the object's components. The list updates as you type to display matching objects.

Step 3 Click **Add to Source**, or drag and drop.

Step 4 Add any source IP addresses or address blocks that you want to specify manually. Click the **Enter an IP address** prompt below the **Source Networks** list; then type an IP address or address block and click **Add**.

Step 5 Click the **DNS** tab and add the lists or feeds that include the DNS names you are controlling. For more information, see Control traffic based on DNS list or feed, on page 16.

Step 6 Save or continue editing the rule.

The DNS rule is configured with network conditions to control traffic based on the specified source IP addresses and DNS names.

What to do next

- Deploy configuration changes.

Control traffic based on DNS and VLAN

This task allows you to control VLAN-tagged traffic by configuring VLAN conditions in DNS rules, enabling precise traffic management based on DNS names and VLAN identifiers.

VLAN conditions in DNS rules allow you to control VLAN-tagged traffic. The system uses the innermost VLAN tag to identify a packet by VLAN.

When you build a VLAN-based DNS rule condition, you can manually specify VLAN tags. Alternately, you can configure VLAN conditions with VLAN tag *objects*, which are reusable and associate a name with one or more VLAN tags.

Procedure

Step 1 In the DNS rule editor, select **VLAN Tags**.

Step 2 Find and select the VLANs you want to add from the **Available VLAN Tags**, as follows:

- To add a VLAN tag object on the fly, which you can then add to the condition, click **Add** (+) above the Available VLAN Tags list and proceed as described in Create a VLAN tag object.
- To search for VLAN tag objects and groups to add, click the **Search by name or value** prompt above the **Available VLAN Tags** list, then type either the name of the object, or the value of a VLAN tag in the object. The list updates as you type to display matching objects.

Step 3 Click **Add to Rule**, or drag and drop.

Step 4 Add any VLAN tags that you want to specify manually. Click the **Enter a VLAN Tag** prompt below the **Selected VLAN Tags** list; then type a VLAN tag or range and click **Add**. You can specify any VLAN tag from 1 to 4094; use a hyphen to specify a range of VLAN tags.

Step 5 Click the **DNS** tab and add the lists or feeds that include the DNS names you are controlling. For more information, see Control traffic based on DNS list or feed, on page 16.

Step 6 Save or continue editing the rule.

The DNS rule is configured with VLAN conditions, allowing the system to control traffic based on both DNS names and VLAN tags.

What to do next

- Deploy configuration changes.

Control traffic based on DNS list or feed

Control network traffic by applying DNS-based filtering rules using predefined or custom DNS lists and threat intelligence feeds.

Use DNS lists and feeds in security policies to block or allow traffic based on domain reputation and threat intelligence data.

Procedure

Step 1 In the DNS rule editor, click **DNS**.

Step 2 Find and select the DNS lists and feeds you want to add from the **DNS Lists and Feeds**, as follows:

- To add a DNS list or feed on the fly, which you can then add to the condition, click **Add** (+) above the **DNS Lists and Feeds** list and proceed as described in Create custom security intelligence feeds.
- To search for DNS lists, feeds, or categories to add, click the **Search by name or value** prompt above the **DNS Lists and Feeds** list, then type an object name or the value of one of the object's components. The list updates as you type to display matching objects.
- For descriptions of the system-provided threat categories, see Security intelligence categories.

Step 3 Click **Add to Rule**, or drag and drop.

Step 4 Save or continue editing the rule.

The DNS lists and feeds are now configured in your rule and will filter traffic based on the selected criteria.

What to do next

- Deploy configuration changes.

Controlling traffic based on security group tag or dynamic attributes

This task allows you to control traffic using dynamic attributes conditions in DNS rules based on security group tags or other dynamic attributes.

Dynamic Attributes conditions in DNS rules allow you to control traffic based on security group tag or other dynamic attributes. To use these attributes, you must apply security group tags to traffic in your network, or create the dynamic attribute objects you need using the API or the Cisco Secure Dynamic Attributes Connector. For more information about enabling dynamic attributes, see Dynamic attributes rule conditions, on page 13.

When you configure dynamic attributes for a DNS rule, objects of the same type in the same source or destination list are ORed together and objects of different types are ANDed together. For example, if you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originates from (or is destined to) one of those IP addresses.

Procedure

Step 1 In the DNS rule editor, click **Dynamic Attributes**.

Step 2 Select the objects you want to use, and click either **Add Sources** or **Add Destinations**.

Initially, all **Dynamic Objects** and **Security Group Tags** are listed when you open the **Dynamic Attributes** tab. You can deselect an option to remove those objects from the list. You can also start typing in the search box to find the object you want.

You can use these objects to identify the source of the connection, the destination, or both.



Note You can use SGT and endpoint device type objects as source criteria only.

Step 3 Click the **DNS** tab and add the lists or feeds that include the DNS names you are controlling. For more information, see Control traffic based on DNS list or feed, on page 16.

Step 4 Save or continue editing the rule.

You have successfully configured dynamic attributes for DNS rules to control traffic based on security group tags or other dynamic attributes.

What to do next

- Deploy configuration changes.

Use a DNS sinkhole to enforce content restriction

This task configures a DNS sinkhole to redirect traffic to the Google SafeSearch Virtual IP Address (VIP), which imposes content filters on Google and YouTube search results.

Typically, a DNS sinkhole directs traffic away from a particular target. This procedure describes how to configure a DNS sinkhole to redirect traffic to the Google SafeSearch Virtual IP Address (VIP), which imposes content filters on Google and YouTube search results.

Because Google SafeSearch uses a single IPv4 address for the VIP, hosts must use IPv4 addressing.



Caution If your network includes proxy servers, this content restriction method is not effective unless you position your Firewall Threat Defense devices between the proxy servers and the Internet.

This procedure enforces content restriction for Google searches only. It does not apply to any other search engine.

Before you begin

This procedure applies to Firewall Threat Defense only, and requires the IPS license.

Follow these steps to use a DNS sinkhole to enforce content restriction:

Procedure

Step 1 Obtain a list of supported Google domains via the following URL: https://www.google.com/supported_domains.

Step 2 Create a custom DNS list on your local computer, and add the following entries:

- To enforce Google SafeSearch, add an entry for each supported Google domain.
- To enforce YouTube Restricted Mode, add a "youtube.com" entry.

The custom DNS list must be in text file (.txt) format. Each line of the text file must specify an individual domain name, stripped of any leading periods. For example, the supported domain ".google.com" must appear as "google.com".

Step 3 Upload the custom DNS list to the Cloud-Delivered Firewall Management Center; see Upload new custom security intelligence lists to the Cloud-Delivered Firewall Management Center.

Step 4 Determine the IPv4 address for the Google SafeSearch VIP. For example, run **nslookup** on forcesafesearch.google.com.

Step 5 Create a sinkhole object for the SafeSearch VIP; see Create a sinkhole object.

Use the following values for this object:

- IPv4 Address—Enter the SafeSearch VIP address.
- IPv6 Address—Enter the IPv6 loopback address (**::1**).
- Log Connections to Sinkhole—Click Log Connections.
- Type—Choose **None**.

Step 6 Create a basic DNS policy; see Create basic DNS policies, on page 5.

Step 7 Add a DNS rule for the sinkhole; see Create and edit DNS rules, on page 7.

For this rule:

- Check the **Enabled** check box.
- Choose **Sinkhole** from the **Action** drop-down list.
- Choose the sinkhole object you created from the **Sinkhole** drop-down list.
- Add the custom DNS list you created to the **Selected Items** list on **DNS**.
- (Optional) Choose a network in **Networks** to limit content restriction to specific users. For example, if you want to limit content restriction to student users, assign students to a different subnet than faculty, and specify that subnet in this rule.

Step 8 Associate the DNS policy with an access control policy; see Associate prefilter, decryption, and identity policies with an access control.

Step 9 Deploy configuration changes.

The DNS sinkhole is configured to enforce content restriction by redirecting traffic to the Google SafeSearch VIP, which filters Google and YouTube search results.

Requirement: deploy DNS policy configuration changes

After you finish updating your DNS policy configuration, you must deploy it as part of access control configuration.

- Associate your DNS policy with an access control policy, as described in Configure security intelligence.
- Deploy configuration changes.

Cisco umbrella DNS policies

A Cisco Umbrella DNS policy is a security mechanism that

- redirects DNS queries to Cisco Umbrella for domain validation and policy enforcement,
- allows or blocks requests based on domain names and applies DNS-based security policies, and
- provides two lines of protection through local DNS inspection and cloud-based Cisco Umbrella policies.

DNS query redirection process

Cisco Umbrella DNS Connection in the management center helps to redirect DNS queries to Cisco Umbrella. This allows Cisco Umbrella to validate requests, allow or block them based on the domain names, and apply DNS-based security policy on the request. If you use Cisco Umbrella, you must configure the Cisco Umbrella Connection (**Integrations** > **Cloud Services** and choose the **Cisco Umbrella Connection**) to redirect DNS queries to Cisco Umbrella.

The Umbrella Connector is part of the system's DNS inspection. If your existing DNS inspection policy map decides to block or drop a request based on your DNS inspection settings, the request is not forwarded to Cisco Umbrella. Thus, you have two lines of protection:

- Your local DNS inspection policy
- Your Cisco Umbrella cloud-based policy

When redirecting DNS lookup requests to Cisco Umbrella, the Umbrella Connector adds an EDNS (Extension mechanisms for DNS) record. An EDNS record includes the device identifier information, organization ID, and client IP address. Your cloud-based policy can use those criteria to control access in addition to the reputation of the FQDN. You can also elect to encrypt the DNS request using DNSCrypt to ensure the privacy of usernames and internal IP addresses.

To redirect DNS requests from the management center to Cisco Umbrella:

1. Configure the Cisco Umbrella connection settings.
2. Create and configure an Umbrella DNS policy.
3. Associate the Umbrella DNS policy with an access control policy.
4. Deploy the changes.

For detailed information about how to set up the Umbrella DNS Connector in the management center, see Configuring the Umbrella DNS Connector for Cisco Secure Firewall Management Center.

Redirect DNS requests to Cisco umbrella

Redirect DNS requests from the device to Cisco Umbrella for enhanced security and DNS filtering capabilities.

Use this procedure when you need to configure DNS redirection to Cisco Umbrella using the Cloud-Delivered Firewall Management Center.

Procedure

Step 1 Ensure that you meet the prerequisites.

Prerequisites for configure the umbrella DNS connector, on page 20

Step 2 Configure the Cisco Umbrella connection settings.

Configure Cisco umbrella connection settings, on page 21

Step 3 Create an Umbrella DNS policy.

Create an umbrella DNS policy, on page 22

Step 4 Configure the Umbrella DNS policy.

Edit Umbrella DNS policies and rules, on page 23

Step 5 Associate the Umbrella DNS policy with an access control policy.

Associate the umbrella DNS policy with an access control policy, on page 24

DNS requests from the device are now redirected to Cisco Umbrella for processing and security filtering.

Prerequisites for configure the umbrella DNS connector

This reference provides the prerequisites that must be met before configuring the Umbrella DNS Connector, including minimum platform requirements, account setup, certificate management, and network connectivity requirements.

Table 1: Minimum supported platforms

Product	Version
Secure Firewall Threat Defense	6.6 and above
Cloud-Delivered Firewall Management Center	7.2 and above

- Establish an account with Cisco Umbrella at https://umbrella.cisco.com, and log into Umbrella at http://login.umbrella.com.
- Import the CA certificate from the Cisco Umbrella server to the Cloud-Delivered Firewall Management Center. In Cisco Umbrella, choose **Deployments** > **Configuration** > **Root Certificate** and download the certificate.

You must import the root certificate to establish the HTTPS connection with the Cisco Umbrella registration server. The certificate needs to be trusted for SSL server validation, which is a non-default option in the Cloud-Delivered Firewall Management Center. Copy and paste this certificate for the device in the Cloud-Delivered Firewall Management Center(**Devices** > **Certificates**).

```
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
SaZMkE4f97Q=
```

When you add the certificate in the management center, ensure that you check the **CA Only** check box.

- Install the certificate on the device.
- Obtain this data from Umbrella:
  - Organization ID
  - Network Device Key
  - Network Device Secret
  - Legacy Network Device Token
- Ensure that the Cloud-Delivered Firewall Management Center is connected to the internet.
- Ensure that the base license with the export-controlled feature option is enabled in the Cloud-Delivered Firewall Management Center.
- Ensure that the DNS server is configured to resolve api.opendns.com.
- Ensure that the Cloud-Delivered Firewall Management Center can resolve management.api.umbrella.com for policy configuration.
- Configure the Firewall Threat Defense route to api.opendns.com.

Configure Cisco umbrella connection settings

Configure the token and settings required to register the device with Cisco Umbrella and enable DNS security services.

The Cisco Umbrella Connection settings define the token that is needed to register the device with Cisco Umbrella.

Before you begin

Establish an account with Cisco Umbrella https://umbrella.cisco.com, and then log into Umbrella at https://dashboard.umbrella.com and obtain the required information to establish connection to Cisco Umbrella.

Follow these steps to configure Cisco Umbrella connection settings:

Procedure

Step 1 Choose **Integrations** > **Cloud Services** and choose the **Cisco Umbrella Connection**.

Step 2 Obtain the following details and add them to the **General** settings:

- **Organization ID**—A unique number that identifies your organization on Cisco Umbrella. Every Umbrella organization is a separate instance of Umbrella and has its own dashboard. Organizations are identified by their name and their organization ID (Org ID).
- **Network Device Key**—The key to fetch umbrella policy from Cisco Umbrella.
- **Network Device Secret**—The secret to fetch umbrella policy from Cisco Umbrella.
- **Legacy Network Device Token**—An Umbrella Legacy Network Devices API token is issued through the Cisco Umbrella dashboard. Umbrella requires the API token to register a network device.

Step 3 Under **Advanced**, configure the following optional settings:

- **DNSCrypt Public Key**—DNSCrypt authenticates and encrypts the DNS queries between the endpoint and the DNS server. To enable DNScrypt, you can configure the DNScrypt public key for certificate verification. The key is a 32-byte hexadecimal value and 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 Umbrella Anycast servers.
- **Management Key**—A key to fetch datacenter details from Umbrella cloud for VPN policy.
- **Management Secret**—A secret used to fetch datacenters from Umbrella cloud for VPN.

Step 4 Click **Test Connection**—Test if the Cisco Umbrella Cloud is reachable from the Cloud-Delivered Firewall Management Center. When you provide the required organization ID and network device details, the umbrella connection is created.

Step 5 Click **Save**.

The Cisco Umbrella connection is configured and the device is ready to register with Cisco Umbrella using the specified credentials and settings.

Create an umbrella DNS policy

Create an Umbrella DNS policy to implement DNS-based security controls and filtering for network protection.

Umbrella DNS policies provide DNS security by blocking malicious domains and controlling access to web content through DNS filtering.

Before you begin

Follow these steps to create an Umbrella DNS policy:

Procedure

Step 1 Choose **Policies** > **Security policies** > **DNS**.

Step 2 Click **Add DNS Policy** > **Umbrella DNS Policy**.

Step 3 Give the policy a unique **Name** and, optionally, a **Description**.

Step 4 Click **Save**.

The Umbrella DNS policy is created and ready for configuration with DNS security rules.

What to do next

Configure the policy. See Edit Umbrella DNS policies and rules, on page 23.

Edit Umbrella DNS policies and rules

Edit Umbrella DNS policies and rules to modify protection policies, configure bypass domains, enable DNSCrypt encryption, and adjust connection timeout settings to meet your organization's specific DNS security requirements.

Use this procedure when you need to modify existing Umbrella DNS policies and their associated rules. You can update protection policy settings, configure local domain bypasses, enable encryption options, and adjust timeout parameters to optimize DNS security for your network environment.

Procedure

Step 1 Choose **Policies** > **Security policies** > **DNS**.

Step 2 In the DNS Policy page, select the Umbrella DNS policy that you want to edit and click **Edit** ( ).

Refresh the Umbrella Protection Policy

If you want to get the latest Umbrella Protection Policy from Cisco Umbrella, click the **Refresh** icon next to **Umbrella Protection Policy Last Updated**.

To configure or modify Umbrella Connection settings for the Management Center, go to **Integrations** > **Cloud Services** Choose the **Cisco Umbrella Connection**.

Step 3 In the Umbrella DNS policy editor, select the Umbrella DNS rule and click **Edit** ( ).

Step 4 Configure the rule components, or accept the defaults:

- **Umbrella Protection Policy**—Specify the name of the Cisco Umbrella policy to apply to the device.
- **Bypass Domain**—Specify the name of the local domains for which DNS requests should bypass Cisco Umbrella and instead go directly to the configured DNS servers.

For example, you can have your internal DNS server resolve all names for the organization's domain name on the assumption that all internal connections are allowed.

- **DNSCrypt**— Enable DNSCrypt to encrypt connections between the device and Cisco Umbrella.

  Enabling DNScrypt starts the key-exchange thread with the Umbrella resolver. The key-exchange thread performs the handshake with the resolver every hour and updates the device with a new secret key. As DNScrypt uses UDP/443, you must ensure that the class map used for DNS inspection includes that port. Note that the default inspection class already includes UDP/443 for DNS inspection.

- **Idle Timeout**—Configure the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.

Step 5 Click **Save**.

Your Umbrella DNS policy and rule modifications are saved and ready to be deployed. The updated settings will take effect when the policy is applied to devices.

What to do next

Associate the Umbrella DNS policy with an access control policy. For more information, see Associate the umbrella DNS policy with an access control policy, on page 24.

Associate the umbrella DNS policy with an access control policy

This task associates an Umbrella DNS policy with an access control policy to enable DNS-based security intelligence filtering before deploying the policy on the device.

Before you deploy the Umbrella DNS policy on the device, you must associate it with an access control policy.

Procedure

Step 1 Choose **Policies** > **Security policies** > **Access Control** and select the access policy to edit.

Step 2 Select **Security Intelligence**.

Step 3 From the **Umbrella DNS Policy** drop-down list, select the Umbrella DNS policy.

Step 4 Click **Save**.

The Umbrella DNS policy is now associated with the access control policy and will provide DNS-based security intelligence filtering when deployed.

What to do next

Deploy configuration changes; see Deploy configuration changes.

DNS over HTTPs and QUIC

Cisco Secure Firewall enables visibility and control over DNS traffic that uses encryption protocols, including DNS over HTTPS (DoH), and DNS over QUIC (DoQ).

As browsers and operating systems increasingly adopt encrypted DNS protocols, traditional DNS inspection faces visibility gaps. You can use this feature to inspect encrypted DNS traffic over HTTPS (HTTP/1.1, HTTP/2, HTTP/3) and QUIC streams. This allows you to apply DNS Security Intelligence and enforce policies, so you can maintain compliance and protection without compromising privacy

Note Decryption policy must be configured to inspect DoH and DoQ.

Limitations

- **Sinkhole support**: Sinkhole actions support only Type A and AAAA records. For other record types, the connection is closed without an injected packet.
- **Injection**: Firewall Threat Defense injects a DNS reply for the "Sinkhole" action and "NX Domain". These injections are not supported for DNS over HTTP/3 and DNS over QUIC. These injections will behave the same as a "Block" action.

Configure DNS over HTTPs or QUIC

Enable Security Intelligence inspection for DNS over HTTPS (DoH) and DNS over QUIC (DoQ) to protect against malicious domains.

This task helps you apply DNS filtering and sinkholing for encrypted DNS traffic, ensuring your network is protected using Security Intelligence policies.

Before you begin

Before you configure the feature, make sure these requirements are met:

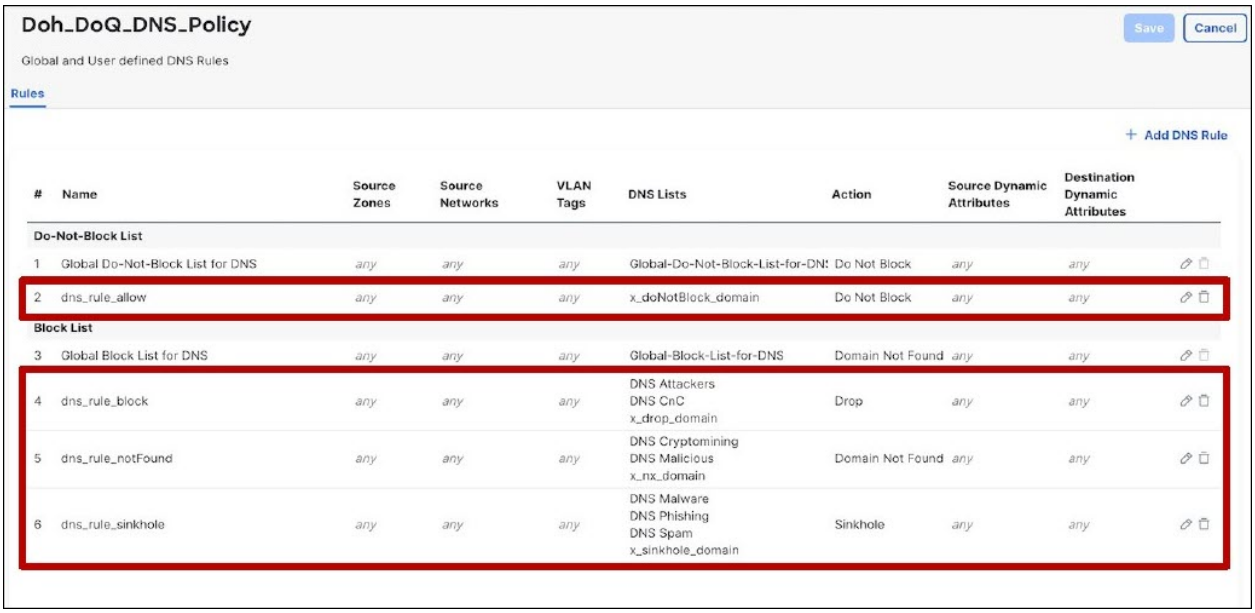
- **DNS infrastructure**: Internal or public DNS servers must be reachable.
- **Client configuration**: Browsers or clients must have Secure DNS enabled.
- **Talos feed**: Ensure the DNS Security Intelligence feed is updated and synchronized from the Talos cloud.

Procedure

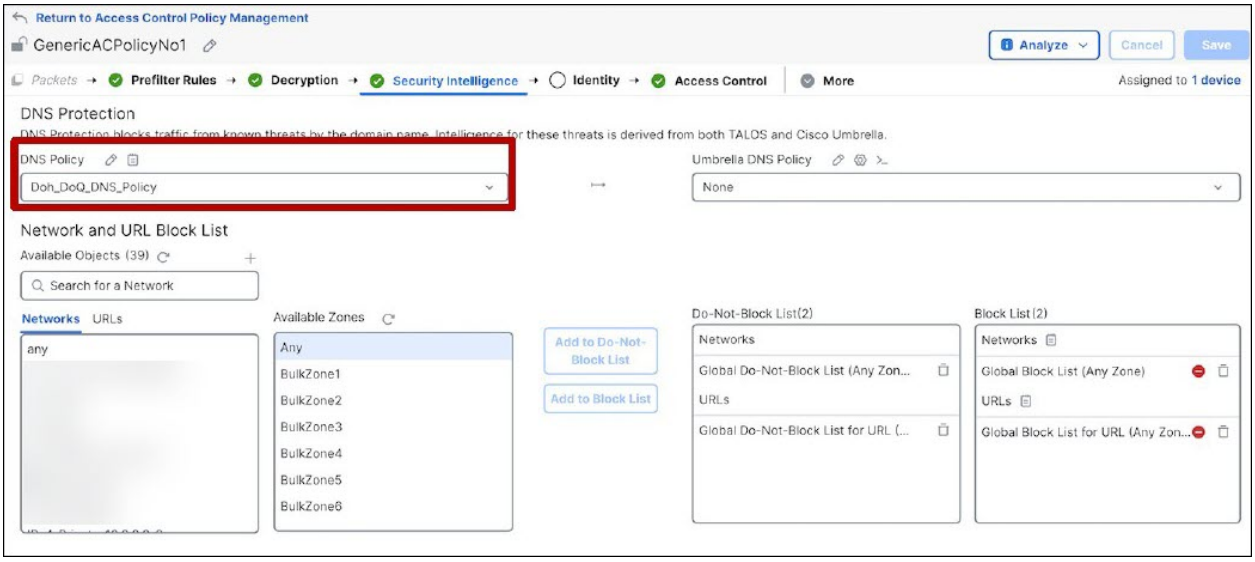
Step 1 Choose **Objects** > **Security Intelligence** > **DNS Lists and Feeds** and create DNS lists for custom actions such as Do Not Block, Drop, Domain Not Found, and Sinkhole.

Step 2 Choose **Objects** > **Sinkhole** and configure a sinkhole object by specifying IPv4 and IPv6 addresses.

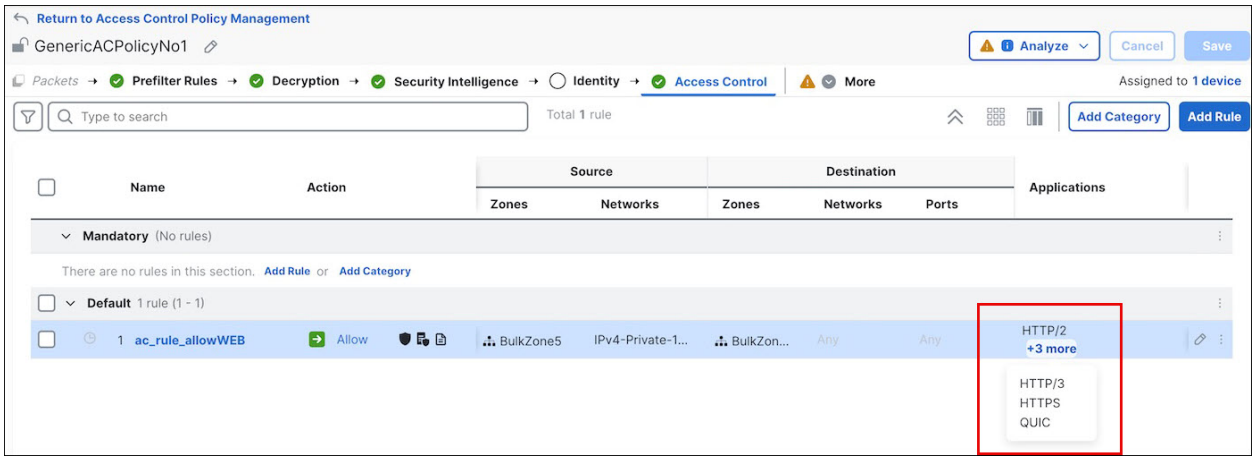
Step 3 Choose **Policies** > **Security policies** > **DNS** and create a new policy and add DNS rules that map the DNS lists created in Step 1.



Step 4 Choose **Policies** > **Security policies** > **Access Control** and associate the DNS policy with your access control policy under the **Security Intelligence** tab.



Step 5 In the access control policy editor, add rules to allow applications such as HTTPS, HTTP/2, HTTP/3, and QUIC, ensuring DNS traffic is inspected.



Step 6 Save and deploy the policy to the Firewall Threat Defense device.

DNS over HTTPS and QUIC monitoring and verification

To monitor and verify DNS traffic for HTTPS and QUIC protocols:

- Execute `show snort counters` on the Firewall Threat Defense CLI to view statistics for the modules `dns`, `http_inspect`, `http2_inspect`, `http3_inspect`, and `quic_inspect`.
- Execute `show snort counters` on the Firewall Threat Defense CLI and monitor the telemetry fields `dnsOverUDP`, `dnsOverTCP`,`dnsOverHttp1`, `dnsOverHttp2`, `dnsOverHttp3`, and `dnsOverQuic` to track the usage of different DNS query methods.

DNS over HTTPS and QUIC troubleshooting steps

If your DNS Security Intelligence policy rules do not trigger as expected, do these steps:

- Verify Talos feeds: Verify DNS resolution and HTTPs connectivity to Talos servers.
- Check decryption: Confirm that the Decryption Policy is correctly applied and that the traffic flow is being intercepted.