



DNS Policies

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

- [DNS Policy Overview, page 1](#)
- [DNS Policy Components, page 2](#)
- [DNS Rules, page 5](#)
- [DNS Policy Deploy, page 13](#)

DNS Policy Overview

DNS-based Security Intelligence allows you to whitelist or blacklist traffic based on the domain name requested by a client. Cisco provides domain name intelligence you can use to filter your traffic; you can also configure custom lists and feeds of domain names tailored to your deployment. DNS-based Security Intelligence filtering takes place after hardware-level handling (such as fast-path) and traffic decryption, and before most other policy-based inspection, analysis, or traffic handling.

Traffic blacklisted by a DNS policy 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 override blacklisting with whitelisting to 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 blacklisted, but also logs the match to the blacklist 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.

DNS Policy Components

A DNS policy allows you to whitelist or blacklist connections based on domain name. The following list describes the configurations you can change after creating a DNS policy.

Name and Description

Each DNS policy must have a unique name. A description is optional.

In a multidomain deployment, policy names must be unique within the domain hierarchy. The system may identify a conflict with the name of a policy you cannot view in your current domain.

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 DNS Whitelist rule and a default Global DNS Blacklist rule. Both rules are fixed to the first position in their respective categories. You cannot modify these rules, but you can disable them.

In a multidomain deployment, the system also adds Descendant DNS Whitelists and Descendant DNS Blacklists rules to DNS policies in ancestor domains. These rules are fixed to the second position in their respective categories.



Note If multitenancy is enabled for your Firepower 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 whitelisted or blacklisted by Firepower System subdomain users. From an ancestor domain, you cannot view the contents of descendant lists. If you do not want subdomain users to whitelist or blacklist domains:

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

The system evaluates rules in the following order:

- Global DNS Whitelist rule (if enabled)
- Descendant DNS Whitelists rule (if enabled)
- Whitelist rules
- Global DNS Blacklist rule (if enabled)
- Descendant DNS Blacklists rule (if enabled)
- Blacklist and Monitor rules

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.

Creating Basic DNS Policies

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

Procedure

- Step 1** Choose **Policies > Access Control > DNS**.
- Step 2** Click **Add DNS Policy**.
- Step 3** Give the policy a unique **Name** and, optionally, a **Description**.
- Step 4** Click **Save**.
-

What to Do Next

- Optionally, further configure the new policy as described in [Logging Blacklisted Connections](#).
- Deploy configuration changes; see [Deploying Configuration Changes](#).



Editing DNS Policies

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

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 > Access Control > DNS**.
- Step 2** Click the edit icon () next to the DNS policy you want to edit.
- If a view icon () 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 the **Rules** tab and proceed as described in [Creating and Editing DNS Rules](#), on page 6.
- Step 4** Click **Save**.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Managing DNS Policies

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin




Use the DNS Policy page (**Policies > Access Control > DNS**) to manage custom DNS policies. In addition to custom policies that you create, the system provides the Default DNS Policy, which uses the default blacklist and whitelist. You can edit and use this system-provided custom policy. In a multidomain deployment, this default policy uses the default Global DNS Blacklist, Global DNS Whitelist, Descendant DNS Blacklists, and Descendant DNS Whitelists, and can only be edited in the Global domain.

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Procedure

Step 1 Choose **Policies > Access Control > DNS**.

Step 2 Manage your DNS policy:

- Copy — To copy a DNS policy, click the copy icon () and proceed as described in [Editing DNS Policies, on page 4](#).
- Create — To create a new DNS policy, click **Add DNS Policy** and proceed as described in [Creating Basic DNS Policies, on page 3](#).
- Delete — To delete a DNS policy, click the delete icon () , then confirm you want to delete the policy.
- Edit — To modify an existing DNS policy, click the edit icon () and proceed as described in [Editing DNS Policies, on page 4](#)

DNS Rules

DNS rules handle traffic based on the domain name requested by a host. As part of Security Intelligence, this evaluation happens after any traffic decryption, and before access control evaluation.

The system matches traffic to DNS rules in the order you specify. In most cases, the system handles network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic. When you create DNS rules, the system places whitelist rules before monitor and blacklist rules, and evaluates traffic against whitelist rules first.

In addition to its unique name, each DNS rule has the following 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, or VLAN.

Action

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

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

Creating and Editing DNS Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

In a DNS policy, you can add up to a total of 32767 DNS lists to the whitelist and blacklist rules. That is, the number of lists in the DNS policy cannot exceed 32767.

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 the edit icon (✎).

Step 2 Enter a **Name**.

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

- Action —Select a rule **Action**; see [DNS Rule Actions](#), on page 8.
- Conditions — Configure the rule's conditions; see [DNS Rule Conditions](#), on page 10.
- Enabled — Specify whether the rule is **Enabled**.

Step 4 Click **Save**.

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

DNS Rule Management

The **Rules** tab of the DNS policy editor allows you to add, edit, move, enable, disable, delete, and otherwise manage DNS rules within your policy.

For each rule, the policy editor displays its name, a summary of its conditions, and the rule action. Other icons represent warnings (⚠), errors (❗), and other important information (ℹ). Disabled rules are dimmed and marked (disabled) beneath the rule name.

Enabling and Disabling DNS Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

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.

Procedure

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

Step 2 Click **Save**.

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

DNS Rule Order Evaluation

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. In most cases, the system handles network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic:

- For Monitor rules, the system logs the traffic, then continues evaluating traffic against lower-priority DNS blacklist 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.

Note the following regarding rule order:

- The Global Whitelist is always first, and takes precedence over all other rules.
- The Descendant DNS Whitelists rule only appears in multidomain deployments, in non-leaf domains. It is always second, and takes precedence over all other rules except the Global Whitelist.
- The Whitelist section precedes the Blacklist section; whitelist rules always take precedence over other rules.
- The Global Blacklist is always first in the Blacklist section, and takes precedence over all other Monitor and blacklist rules.
- The Descendant DNS Blacklists rule only appears in multidomain deployments, in non-leaf domains. It is always second in the Blacklist section, and takes precedence over all other Monitor and blacklist rules except the Global Blacklist.
- The Blacklist section contains Monitor and blacklist rules.
- When you first create a DNS rule, the system positions it last in the Whitelist section if you assign a **Whitelist** action, or last in the Blacklist section if you assign any other action.

You can drag and drop rules to reorder them.

DNS Rule Actions

Every DNS rule has an *action* that determines the following for matching traffic:

- handling—foremost, the rule action governs whether the system will whitelist, monitor, or blacklist traffic that matches the rule's conditions
- logging—the rule action determines when and how you can log details about matching traffic

Keep in mind that only devices deployed inline can blacklist traffic. Devices deployed passively or in tap mode can whitelist and log, but not affect, traffic.

Whitelist Action

The **Whitelist** action allows matching traffic to pass. When you whitelist traffic, it is subject to further inspection either by a matching access control rule, or the access control policy's default action.

The system does not log whitelist matches. However, logging of whitelisted connections depends on their eventual disposition.

Monitor Action

The **Monitor** action does not affect traffic flow; matching traffic is neither immediately whitelisted nor blacklisted. Rather, 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 blacklists 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 Firepower Management Center database.

Blacklist Actions

The blacklist actions blacklist traffic without further inspection of any kind:

- The **Drop** action drops the traffic.
- The **Domain Not Found** action returns a non-existent internet domain response to the DNS query, which prevents the client from resolving the DNS request.
- The **Sinkhole** action returns a sinkhole object's IPv4 or IPv6 address in response to the DNS query. 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.

For a connection blacklisted based on the **Drop** or **Domain Not Found** actions, the system logs beginning-of-connection Security Intelligence and connection events. Because blacklisted traffic is immediately denied without further inspection, there is no unique end of connection to log.

For a connection blacklisted 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.



Note

On an ASA FirePOWER device, if you configure a DNS rule with a sinkhole action, and traffic matches the rule, the ASA blocks the follow-on sinkhole connection by default. As a workaround, run the following commands from the ASA command line:

```
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# no inspect dns preset_dns_map
If the ASA continues to block the connection, contact Support.
```

DNS Rule Conditions

A DNS rule's conditions identify the type of traffic that rule handles. Conditions can be simple or complex. You must define a DNS feed or list condition within a DNS rule. You can also optionally control traffic by security zone, network, 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 blacklist traffic based on up to 50 DNS lists and feeds.

Controlling Traffic Based on DNS and Security Zone

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

Zone conditions in DNS rules allow you to control traffic by its source and destination security zones. A *security zone* is a grouping of one or more interfaces, which may be located across multiple devices. An option you choose during a device's initial setup, called its *detection mode*, determines how the system initially configures the device's interfaces, and whether those interfaces belong to a security zone.

Procedure

-
- Step 1** In the DNS rule editor, click the **Zones** tab.
 - 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** Save or continue editing the rule.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Controlling Traffic Based on DNS and Network

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

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 the **Networks** tab.
- 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 the add icon (+) above the **Available Networks** list and proceed as described in [Creating Network Objects](#).
 - 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**. The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.
- Step 5** Save or continue editing the rule.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Controlling Traffic Based on DNS and VLAN

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

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 the **VLAN Tags** tab.
- 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 the add icon (+) above the Available VLAN Tags list and proceed as described in [Creating VLAN Tag Objects](#).
 - 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.
The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal VLAN tags to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.
- Step 5** Save or continue editing the rule.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Controlling Traffic Based on DNS List, Feed, or Category

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

DNS conditions in DNS rules allow you to control traffic if a DNS list, feed, or category contains the domain name requested by the client. You must define a DNS condition in a DNS rule.

Regardless of whether you add a global or custom whitelist or blacklist to a DNS condition, the system applies the configured rule action to the traffic. For example, if you add the Global Whitelist to a rule, and configure a **Drop** action, the system blacklists all traffic that should have been whitelisted.

Procedure

-
- Step 1** In the DNS rule editor, click the **DNS** tab.
- 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 the add icon (+) above the **DNS Lists and Feeds** list and proceed as described in [Creating 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.
- Step 3** Click **Add to Rule**, or drag and drop.
- Step 4** Save or continue editing the rule.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

DNS Policy Deploy

Smart License	Classic License	Supported Devices	Supported Domains
Threat	Protection	Any	Any

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 [Configuring Security Intelligence](#).
- Deploy configuration changes; see [Deploying Configuration Changes](#).

