DNS Policies

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

- DNS Policy Overview, page 34-1
- DNS Policy Components, page 34-1
- DNS Rules, page 34-2
- DNS Policy Deploy, page 34-8

DNS Policy Overview

License: Any

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 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. 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 ASA FirePOWER module 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.

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

DNS Policy Components

License: Any

A DNS policy allows you to whitelist or blacklist domain name-based connections. 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.

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 ASA FirePOWER module matches traffic to DNS rules in top-down order by ascending rule number.

When you create a DNS policy, the ASA FirePOWER module populates it with a default Global DNS Whitelist rule, and a default Global DNS Blacklist rule. Each rule is fixed to the first position in their respective categories. You cannot modify these rules, but you can disable them. The module evaluates rules in the following order:

- Global DNS Whitelist rule (if enabled)
- whitelist rules
- Global DNS Blacklist rule (if enabled)
- blacklist and monitor rules

Usually, the module handles domain name-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 module continues evaluating the traffic based on the associated access control policy's rules. DNS rule conditions can be simple or complex.

Editing a DNS Policy

License: Protection

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 module discards your changes.

To edit a DNS policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > DNS Policy**.

Step 2 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, page 34-3.

Step 3 Click **Store ASA FirePOWER Changes.**

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

DNS Rules

License: Any

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 ASA FirePOWER module matches traffic to DNS rules in the order you specify. In most cases, the module handles network traffic according to the first DNS rule where all the rule's conditions match the traffic. When you create DNS rules, the module 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 ASA FirePOWER module 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 ASA FirePOWER module 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 or network.

Action

A rule's action determines how the ASA FirePOWER module 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 module 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

License: Protection

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.

To create and edit DNS Rules:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > DNS Policy**.

Step 2 You have the following options:

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

Step 3 Enter a **Name**.

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

- Action - Select a rule **Action**; see DNS Rule Actions, page 34-5.

- Conditions - Configure the rule's conditions; see DNS Rule Conditions, page 34-6.
- Enabled - Specify whether the rule is **Enabled**.

Step 5 Click **Add** or **OK**.

Step 6 Click **Store ASA FirePOWER Changes**.

DNS Rule Management

License: Any

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 ( ). Disabled rules are dimmed and marked (`disabled`) beneath the rule name.

Enabling and Disabling DNS Rules

License: Protection

When you create a DNS rule, it is enabled by default. If you disable a rule, the ASA FirePOWER module 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.

To enable and disable DNS Rules:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > DNS Policy**.

Step 2 In the DNS policy editor that contains the rule you want to enable or disable, right-click the rule and choose a rule state.

Step 3 Click **OK**.

Step 4 Click **Store ASA FirePOWER Changes**.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

DNS Rule Order Evaluation

License: Any

Rules in a DNS policy are numbered, starting at 1. The ASA FirePOWER module matches traffic to DNS rules in top-down order by ascending rule number. In most cases, the module handles network traffic according to the first DNS rule where all the rule's conditions match the traffic:

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

- For non-Monitor rules, the module 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 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 Blacklist section contains Monitor and blacklist rules.
- When you first create a DNS rule, the module 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, and change the evaluation order.

DNS Rule Actions

License: Any

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

- handling—foremost, the rule action governs whether the module 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 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 module 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 module 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 ASA FirePOWER module logs end-of-connection Security Intelligence and connection events.

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 module 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 module logs end-of-connection connection events for the follow-on connection. If you configure your sinkhole object to log and block sinkhole connections, the module logs beginning-of-connection connection events for the follow-on connection, then blocks that connection.

DNS Rule Conditions

License: Any

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. You can additionally control traffic by security zone or network.

When adding conditions to a DNS rule:

- If you do not configure a particular condition for a rule, the module 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 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

License: Protection

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. An option you choose during a device's initial setup, called its detection mode, determines how the module initially configures the device's interfaces, and whether those interfaces belong to a security zone.

To control traffic based on DNS and security zone:

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**.

Tip You can also drag and drop selected zones.

Step 5 Save or continue editing the rule.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

Controlling Traffic Based on DNS and Network

License: Protection

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.

To control traffic based on DNS and network:

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 Working with Network Objects, page 2-3.
- 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**.

Tip You can also drag and drop selected objects.

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 Save or continue editing the rule.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

Controlling Traffic Based on DNS List, Feed, or Category

License: Protection

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 ASA FirePOWER module 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 module blacklists all traffic that should have been whitelisted.

To control traffic based on DNS list, feed, or category:

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 Working with the Intelligence Feed, page 2-6
- 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**.

Tip You can also drag and drop selected objects.

Step 4 Save or continue editing the rule.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

DNS Policy Deploy

License: Any

After you finishing updating your DNS policy configuration, you must deploy it as part of an access control policy for your changes to take effect. You must do the following:

- Associate your DNS policy with an access control policy, as described in Building the Security Intelligence Whitelist and Blacklist, page 5-3.
- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.