Firepower Management Center Configuration Guide

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.

|  |  |
| --- | --- |
| https://www.cisco.com/c/dam/en/us/td/i/templates/note.gif 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.

|  |  |
| --- | --- |
| https://www.cisco.com/c/dam/en/us/td/i/templates/note.gif 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](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/DNS_Policies.html#task_A456C66B7ACF488FB8E74FC4A7F7A516)
* [Editing DNS Policies](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/DNS_Policies.html#task_FEA62FA17C1A4503B46E096862A9F1B8)
* [Managing DNS Policies](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/DNS_Policies.html#task_D4D2113DAA3045E5936C36AE9E173FFB)