FQDN Objects

FQDN Match Object

A Fully Qualified Domain Name (FQDN) Match Object evaluates the Server Name Indication (SNI) associated with TLS-encrypted traffic or the Host header for unencrypted HTTP traffic. It uses the results of the evaluation for rule matching. If the traffic matches all match objects (Address, FQDN, Service) associated with a rule, then the rule is used to process the traffic. To evaluate the FQDN, traffic must be TLS encrypted and contain an SNI in an unencrypted TLS Hello header or be unencrypted HTTP and contain a Host header. The FQDN can be evaluated for traffic that is processed by either a **Forwarding** or **Forward Proxy** rule. The set of FQDNs in the profile is specified as strings representing the full domain or as strings represented by a Perl Compatible Regular Expression (PCRE).

Note The FQDN match object is organized as a table containing user-specified rows (FQDNs).

The rows do not contain log-related actions to perform. This is because FQDN match object is a first-level matching criteria. When you have a clear list of FDQNs that you want to allow, you can use FQDN match objects. After a rule match, if you have categories that you want to allow based on criteria, use FQDN filtering. For more information, see Fully Qualified Domain Name Filter Profile.

The limits for each FQDN match object are as follows:

- Maximum user-specified rows: 254 (Standalone or Group of Standalones)
- Maximum FQDNs per row: 60
- Maximum FQDN character length: 255

When specifying a multilevel domain (for example, `www.example.com`), it's important to escape the `.` character (for example,`www\.example\.com`) otherwise it treats it as a wildcard for any single character.

Standalone vs. Group

A FQDN Match Object can be specified as Type Standalone or Group.

A FQDN Match Standalone Object contains FQDNs. The Object will be applied directly to a set of one or more Policy Ruleset Rules or associated with a FQDN Match Group Object.

A FQDN Match Group Object contains an ordered list of Standalone FQDN Objects that can be defined for different purposes and combined together into a Group Object. The Group Object can be applied directly to a set of one or more Policy Ruleset Rules. Each team can create and manage specific Standalone Profiles. These Standalone Profiles can be combined together into a Group Profile to create hierarchies or different combinations based on use case. An example combination could be a global FQDN list that would apply to everything, a CSP-specific list that would apply to each different CSP, and an application-specific list that would apply to each different application.

Create Standalone FQDN Match Object

Procedure

Step 1 Navigate to **Manage** > **Security Policies** > **FQDNs**.

Step 2 Click **Create**.

Step 3 Provide a Profile Name and Description.

Step 4 Specify the Type as Standalone.

Step 5 Click **Add** to create a new row.

Step 6 Specify individual FQDNs (e.g., www.twitter.com,.*.google.com)

a) Each FQDN is specified as a PCRE (Perl Compatible Regular Expression).

b) Consider escaping the . character else it will be treated as a single character wildcard.

Step 7 (Optional) Specify Decryption Exception for any FQDNs where decryption is not desired or possible. Possible reasons for considering Decryption Exception include:

Step 8 Desire to not inspect encrypted traffic (financial services, defense, health care, etc.).

Step 9 SSO authentication traffic where decryption is not possible.

Step 10 NTLM traffic that cannot be proxied.

Step 11 Click **Save** when completed.

Create Group FQDN Match Object

Procedure

Step 1 Navigate to **Manage** > **Security Policies** > **FQDNs**.

Step 2 Click **Create**.

Step 3 Provide a Profile Name and Description.

Step 4 Specify the Type as Group.

Step 5 Select an initial Standalone Profile (at least one Standalone Profile is required).

Step 6 Specify additional Standalone Profiles.

Step 7 Click **Add FQDN Profile** to create a new row.

Step 8 Select a Standalone Profile.

Step 9 Click **Save** when completed.

Associate the Object

Check this document to create/edit Policy Rules.