Troubleshoot FQDN Objects with Base Domain Not Matching Subdomains in FTD Access Control Policies

Contents

Issue

When configuring Fully Qualified Domain Name (FQDN) objects in Cisco Firewall Threat Defense (FTD) access control policies, base domain entries do not automatically match subdomains. For example, when creating a policy that allows a destination object configured as "example.com", the subdomain "maps.example.com" gets blocked instead of being allowed through the same policy rule. This behavior raises questions about whether base domains can function as wildcards for all subdomains, and what the proper configuration method is for implementing wildcard FQDN matching in FTD policies.

Environment

- FTD version 7.2. Other versions can be also affected.
- FMC version 7.2. Other versions can be also affected.
- FQDN objects configured in access control policies.

Resolution

- The behavior observed is the expected operation of FQDN objects.
- In Cisco FMC the FQDN objects are designed to match exact domain names and do not automatically function as wildcards for subdomains.
- To properly configure subdomain matching, URL Filtering and URL conditions have to be used instead of FQDN objects.

Configuring URL Filtering for Subdomain Matching

To match a domain and all its subdomains in FMC, use these configuration steps:

Step 1. Navigate to Access Control Policy Rule Configuration

In the FMC, navigate to **Policies > Access Control > Access Control Policy > [Your Policy Name] > Rules**.

Step 2. Create or Edit Access Control Rule

Create a new rule or edit an existing access control rule where you want to implement subdomain matching.

Step 3. Configure URL Conditions

In the rule configuration, add URL conditions instead of using FQDN objects. Configure the URL condition to include the base domain with appropriate wildcard syntax to match subdomains.

Step 4. Apply URL Filtering Policy

Ensure that URL filtering is enabled and properly configured within the access control policy to process the URL conditions effectively.

Step 5. Deploy Configuration

Deploy the configuration changes to the target FTD devices to implement the subdomain matching functionality.

Alternative Configuration Methods

If URL filtering is not suitable for the specific use case, consider creating multiple FQDN objects for each subdomain that needs to be explicitly matched, or use network objects with IP address ranges if the domains resolve to predictable IP address spaces.

Cause

FQDN objects in Cisco FMC are designed to perform exact domain name matching rather than wildcard matching. This is the intended behavior of the system. The FQDN object functionality does not include implicit subdomain matching capabilities, which requires the use of URL filtering conditions to achieve the desired subdomain matching behavior.

Related Content

- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214698-understand-fqdn-feature-on-firepower-thr.html
- https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/214505-configure-fqdn-based-object-for-access-c.html
- Cisco bug ID CSCwf000588
- Cisco Technical Support & Downloads