Understand FQDN Feature on Firepower Threat Defense (FMC-Managed)

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Feature Overview
- What about Pre-6.3

Configure

- Network Diagram
- Architecture – Salient Points
- Configuration Steps

Verify

Troubleshoot

- Gather FMC Troubleshoot Files
- Common Issues/Error Messages
- Deployment Failure
- Recommended Troubleshooting Steps
- No Activated FQDN

Q&A

Introduction

This document describes configuration of the FQDN feature (as of v6.3.0) to Firepower Management Center (FMC) and Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of this topics:

- Firepower Management Center

Components Used

The information in this document is based on these software versions:

- Cisco Firepower Threat Defense (FTD) Virtual which runs software version 6.3.0
- Firepower Management Center Virtual (vFMC) which runs software version 6.3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes configuration of the Fully Qualified Domain Name (FQDN) feature introduced by software version 6.3.0 to Firepower Management Center (FMC) and Firepower Threat Defense (FTD). This feature is present in the Cisco Adaptive Security Appliance (ASA) but it was not on the initial software releases of FTD.

Ensure these conditions are met before you configure FQDN objects:

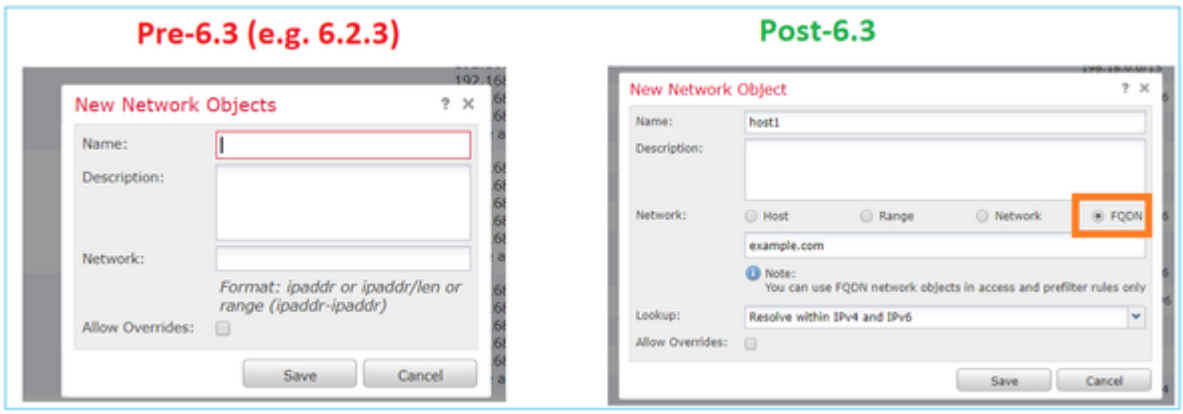
- The Firepower Management Center must run version 6.3.0 or later. It can be physical or virtual
- The Firepower Threat Defense must run version 6.3.0 or later. It can be physical or virtual

Feature Overview

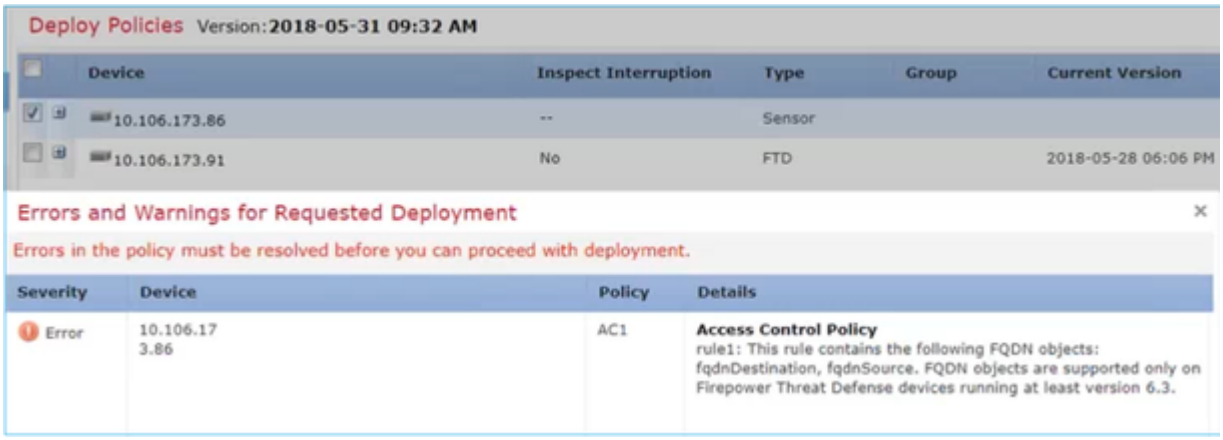
This feature resolves a FQDN into an IP address and uses the latter to filter traffic when referenced by an Access Control Rule or Prefilter Policy.

What about Pre-6.3

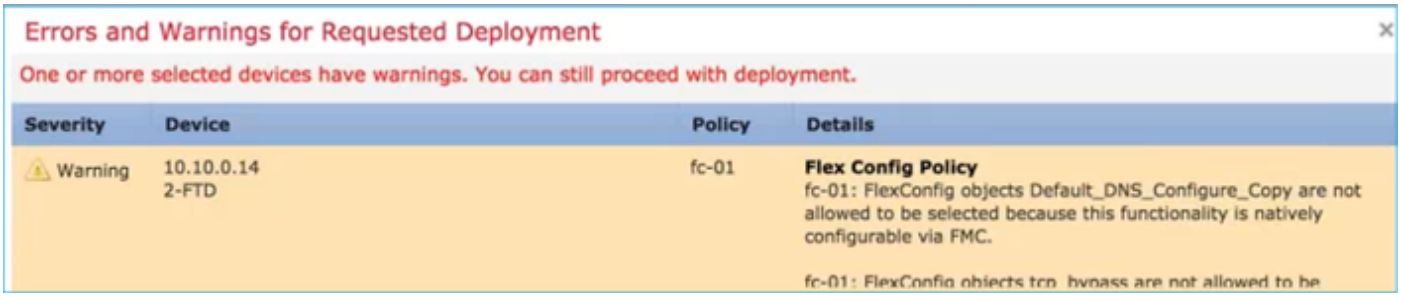
- FMC and FTD which run a version earlier than 6.3.0 cannot configure FQDN objects.



- In case FMC runs version 6.3 or later but FTD runs a version earlier than 6.3, the deployment of a policy shows this error:

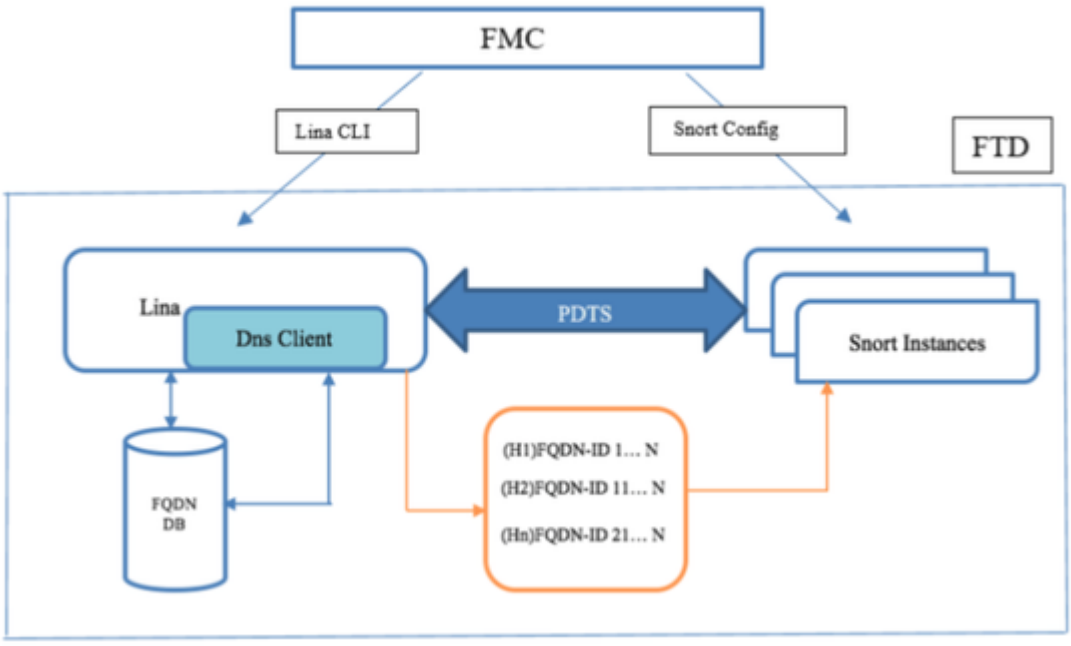


- Additionally, if you configure via FlexConfig a DNS object, this warning appears:



Configure

Network Diagram



Architecture – Salient Points

- DNS resolution (DNS to IP) happens in LINA.
- LINA stores the mapping in its database.
- On a per-connection basis, this mapping is sent from LINA to snort.
- The resolution of FQDN happens independently of High Availability or Cluster configuration.

Configuration Steps

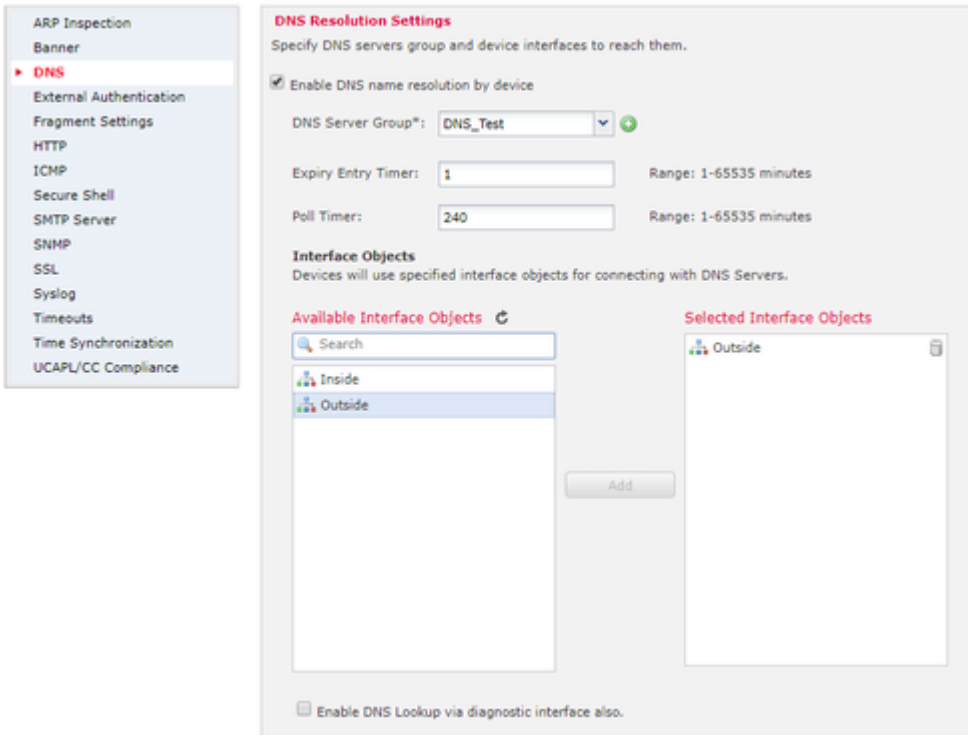
Step 1. Configure the **DNS Server Group Object**.



- DNS server group name must not exceed 63 characters.
- In a multidomain deployment, object names must be unique within the domain hierarchy. The system can identify a conflict with the name of an object you cannot view in your current domain.

- The Default Domain (Optional) is used to append to the hostnames that are not fully-qualified.
- The default Retries and Timeout values are pre-populated.
    - Retries—The number of times, from 0 to 10, to retry the list of DNS servers when the system does not receive a response. The default is 2.
    - Timeout—The number of seconds, from 1 to 30, before another try to the next DNS server. The default is 2 seconds. Each time the system retries the list of servers, this timeout doubles.
- Enter the DNS Servers to be part of this group. This can be either an IPv4 or IPv6 format as comma-separated values.
- The DNS server group is used for resolution with the interface object or objects that are configured in Platform Settings.
- REST API for DNS Server Group object CRUD is supported.

Step 2. Configure **DNS (Platform Settings)**.



- (Optional) Modify the Expiry Entry Timer and Poll Timer values in minutes:

The expiry entry timer option specifies the time limit to remove the IP address of a resolved FQDN from the DNS lookup table after its Time-to-live (TTL) expires. Remove an entry requires the table to be recompiled, so frequent removals can increase the process load on the device. This setting virtually extends the TTL.

The poll timer option specifies the time limit after which the device queries the DNS server to resolve the FQDN that was defined in a network object group. An FQDN is resolved periodically either when the poll timer has expired, or when the TTL of the resolved IP entry has expired, whichever occurs first.

- (Optional) Select the required **interface objects** from the available list and add them to the **Selected Interface Objects** list and ensure the DNS server is reachable through the selected interface(s):

For Firepower Threat Defense 6.3.0 devices, if no interfaces are selected and the diagnostic interface is disabled for DNS lookup, the DNS resolution happens via any interface which includes the diagnostic interface (the command dnsdomain-lookup any is applied).

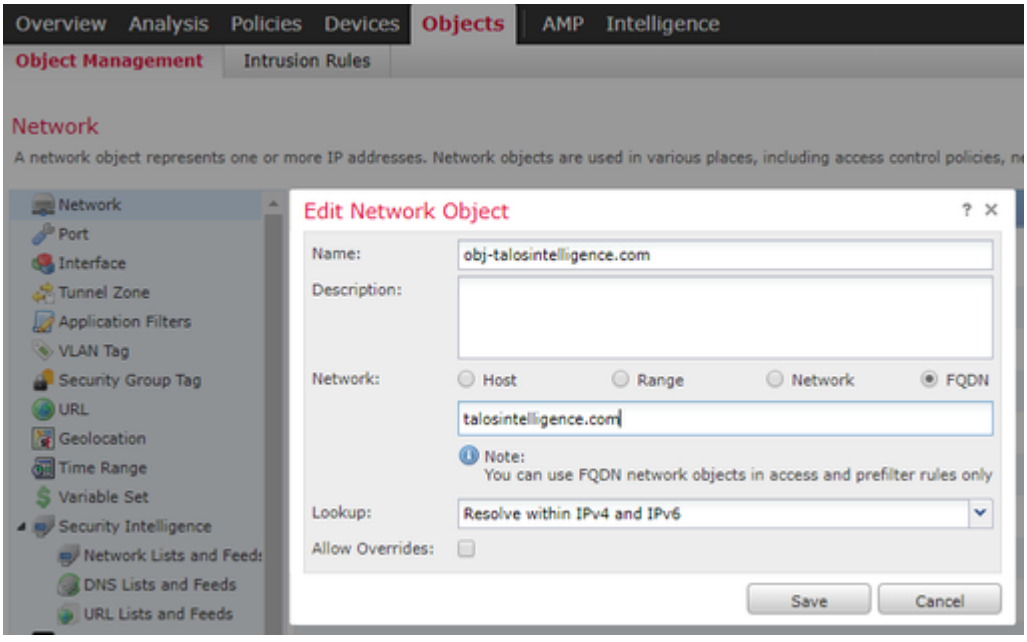
If you do not specify any interfaces—and do not enable DNS lookup on the diagnostic interface, the FTD uses the Data Routing Table to determine the interface. If there is no match, it uses the Management Routing Table.

- (Optional) Select **Enable DNS Lookup** via the diagnostic interface also checkbox.

If enabled, Firepower Threat Defense uses both the selected data interfaces and the diagnostic interface for DNS resolutions. Be sure to configure an IP address for the diagnostic interface on the **Devices > Device Management > edit device > Interfaces page**.

Step 3. Configure the Object Network FQDN

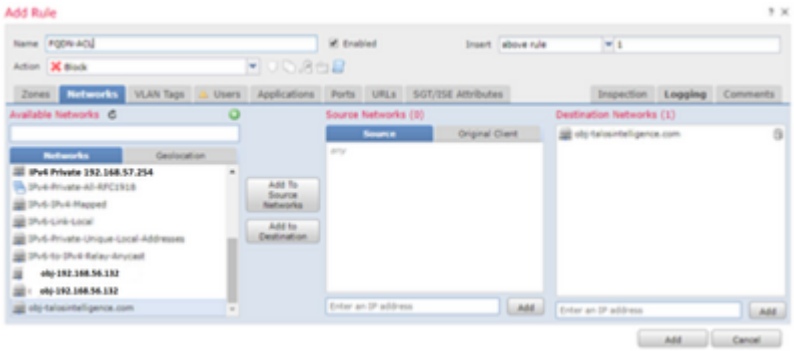
Navigate to **Objects > Object Management**, and within a network object, select the **FQDN** option.

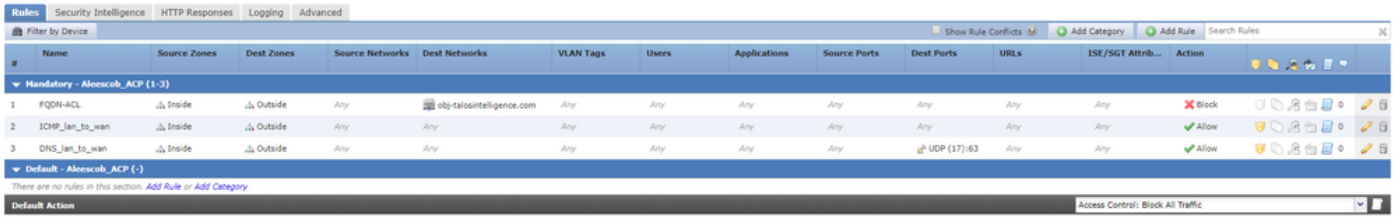


- A 32-bit unique ID gets generated when the user creates an FQDN object.
- This ID is pushed from FMC to both LINA and Snort.
- In LINA this ID is associated with the object.
- In snort, this ID is associated with the access control rule which holds that object.

Step 4. Create an Access Control Rule

Create a rule with the previous FQDN object and deploy the policy:





Note: The first instance of the FQDN resolution occurs when the FQDN object is deployed in an access control policy

Verify

Use this section to confirm your configuration works properly.

- This is the FTD initial configuration before FQDN is deployed:

```
aleescob# show run dns
DNS server-group DefaultDNS
```

- This is the configuration after FQDN deployment:

```
aleescob# show run dns
dns domain-lookup wan_1557
DNS server-group DNS_Test
```

```
    retries 3
    timeout 5
    name-server 172.31.200.100
    domain-name aleescob.cisco.com
DNS server-group DefaultDNS
dns-group DNS_Test
```

- This is how the FQDN object looks in LINA:

```
object network obj-talosintelligence.com
 fqdn talosintelligence.com id 268434436
```

- When it is already deployed, this is how the FQDN access-list looks in LINA:

```
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.co
```

- This is how it looks in Snort (ngfw.rules):

```
# Start of AC rule.
268434437 deny 1 any  any 2 any  any any any  (log dcforward flowstart) (dstfqdn 268434436)
# End rule 268434437
```

Note: In this scenario, since the FQDN object was used for the destination, it is listed as dstfqdn.

- If you check **show dns** and **show fqdn** commands, you notice that the feature has started to resolve the IP for tallosintelligence:

```
aleescob# show dns
Name: talosintelligence.com
  Address: 2001:DB8::6810:1b36                          TTL 00:05:43
  Address: 2001:DB8::6810:1c36                          TTL 00:05:43
  Address: 2001:DB8::6810:1d36                          TTL 00:05:43
  Address: 2001:DB8::6810:1a36                          TTL 00:05:43
  Address: 2001:DB8::6810:1936                          TTL 00:05:43
  Address: 192.168.27.54                                  TTL 00:05:43
  Address: 192.168.29.54                                  TTL 00:05:43
  Address: 192.168.28.54                                  TTL 00:05:43
  Address: 192.168.26.54                                  TTL 00:05:43
  Address: 192.168.25.54                                  TTL 00:05:43
```

```
aleescob# show fqdn
FQDN IP Table:
ip = 2001:DB8::6810:1b36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1c36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1d36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1a36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1936, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.27.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.29.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.28.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.26.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

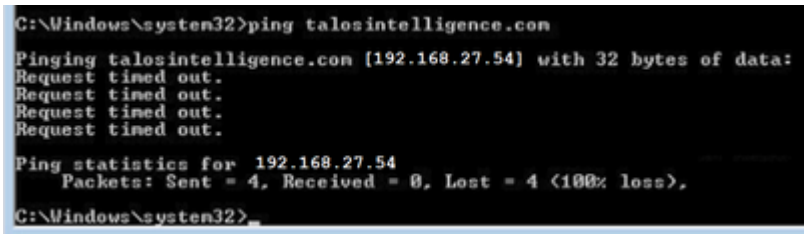
ip = 192.168.25.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

FQDN ID Detail:
FQDN-ID = 268434436, object = obj-talosintelligence.com, domain = talosintelligence.com
        ip = 2001:DB8::6810:1b36, 2001:DB8::6810:1c36, 2001:DB8::6810:1d36, 2001:DB8::6810:1a36, 2001:D
```

- If you check **show access-list** in LINA, you notice the expanded entries for each resolution and hit counts:

```
firepower# show access-list
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintel
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligenc
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (t
```

- As shown in the image, a ping to talosintelligence.com fails since there is a match for the FQDN in the access-list. The DNS resolution has worked since the ICMP packet is blocked by the FTD.



- Hit counts from LINA for the previously sent ICMP packets:

```
access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelli
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligenc
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (t
```

- ICMP requests are captured and shown dropped in the ingress interface:

aleescob# show cap in 13 packets captured 1: 18:03:41.558915 192.168.56.132 > 172.31.200.100 icmp: 192.168.56.132 udp port 59396 unreachable 2: 18:04:12.322126 192.168.56.132 > 172.31.4.161 icmp: echo request 3: 18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp: echo reply 4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp: echo request 5: 18:04:13.462149 172.31.4.161 > 192.168.56.132 icmp: echo reply 6: 18:04:14.308425 192.168.56.132 > 172.31.4.161 icmp: echo request 7: 18:04:14.475424 172.31.4.161> 192.168.56.132 icmp: echo reply 8: 18:04:15.306823 192.168.56.132 > 172.31.4.161 icmp: echo request 9: 18:04:15.463339 172.31.4.161 > 192.168.56.132 icmp: echo reply 10: 18:04:25.713662 192.168.56.132 > 192.168.27.54 icmp: echo request 11: 18:04:30.704232 192.168.56.132 > 192.168.27.54 icmp: echo request 12: 18:04:35.711480 192.168.56.132 > 192.168.27.54 icmp: echo request 13: 18:04:40.707528 192.168.56.132 > 192.168.27.54 icmp: echo request aleescob# sho cap asp | in 192.168.27.54 162: 18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp: echo request 165: 18:04:30.704355 192.168.56.132 > 192.168.27.54 icmp: echo request 168: 18:04:35.711556 192.168.56.132 > 192.168.27.54 icmp: echo request 176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp: echo request.

- This is how the trace looks for one of these ICMP packets:

```
aleescob# sho cap in packet-number 10 trace

13 packets captured

  10: 18:04:25.713662       192.168.56.132 > 192.168.27.54 icmp: echo request
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.57.254 using egress ifc  wan_1557

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.co
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
Additional Information:

Result:
input-interface: lan_v1556
input-status: up
input-line-status: up
output-interface: wan_1557
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

- If the action for the access control rule is Allow, this is an example of the output of system support firewall-engine-debug

```
> system support firewall-engine-debug

Please specify an IP protocol: icmp
Please specify a client IP address: 192.168.56.132
Please specify a server IP address:
Monitoring firewall engine debug messages

192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 new firewall session
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 DAQ returned DST FQDN ID: 268434436
```

```
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Starting with minimum 2, 'FQDN-ACL', and SrcZone first wi
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Match found for FQDN id: 268434436
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 match rule order 2, 'FQDN-ACL', action Allow
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 MidRecovery data sent for rule id: 268434437,rule_action:
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 allow action
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 deleting firewall session
```

- When the FQDN is deployed as part of a Prefilter (Fastpath), this is how it looks in ngfw.rules:

```
iab_mode Off
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268434439 fastpath any any  any any any  any any any  (log dcforward both) (tunnel -1)
268434438 allow any any  1025-65535 any any  3544 any 17  (tunnel -1)
268434438 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268434438 allow any any  any any any  any any 47  (tunnel -1)
268434438 allow any any  any any any  any any 41  (tunnel -1)
268434438 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.
```

- From LINA point of view with a traced packet:

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip any object obj-talosintelligence.com rule-id 268434439 event-
access-list CSM_FW_ACL_ remark rule-id 268434439: PREFILTER POLICY: Prefilter-1
access-list CSM_FW_ACL_ remark rule-id 268434439: RULE: FQDN_Prefilter
Additional Information:
```

Troubleshoot

1. Configuration from FMC

- Verify Policies and the DNS server settings are configured properly.
- Verify the deployment is successful.

2. Deploy Check on FTD

- Run **show dns** and **show access-list** to see if FQDN is resolved and AC rules are expanded.
- Run **show run object network** and note the ID associated with the object (say X for source).

- Run **show fqdn id X** to check if the FQDN is resolved to the source IP properly.
- Verify if the ngfw.rules file has AC rule with FQDN ID X as source.
- Run **system support firewall-engine-debug** and check the Snort verdict.

Gather FMC Troubleshoot Files

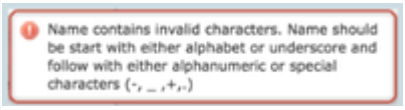
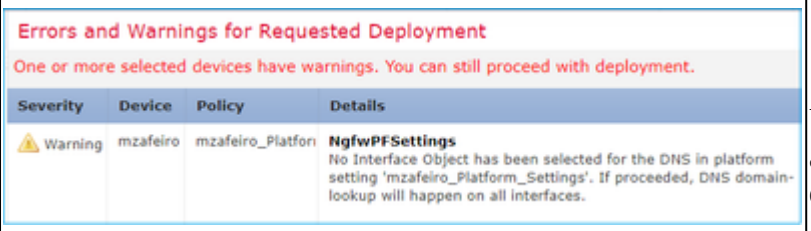
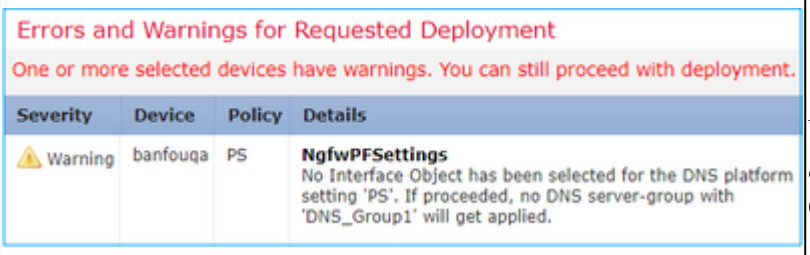
All the logs needed are gathered from an FMC Troubleshoot. To gather all the important logs from FMC, run a Troubleshoot from the FMC GUI. Otherwise, from a FMC Linux prompt, run sf_troubleshoot.pl. If you find an issue, please submit an FMC Troubleshoot with your report to the Cisco Technical Assistance Center (TAC).

FMC Logs

Log File Name/Location	**Purpose**
`/opt/CSCOpx/MDC/log/operation/vmsshareddsvcs.log`	All API Calls
`/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log`	All API Calls
`/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log`	CLI Generation Logs
`/opt/CSCOpx/MDC/tomcat/logs/stdout.log`	Tomcat Logs
`/var/log/mojo.log`	Mojo Logs
`/var/log/CSMAgent.log`	REST Calls between CSM & DC
`/var/log/action_queue.log`	DC’s Action Queue Log

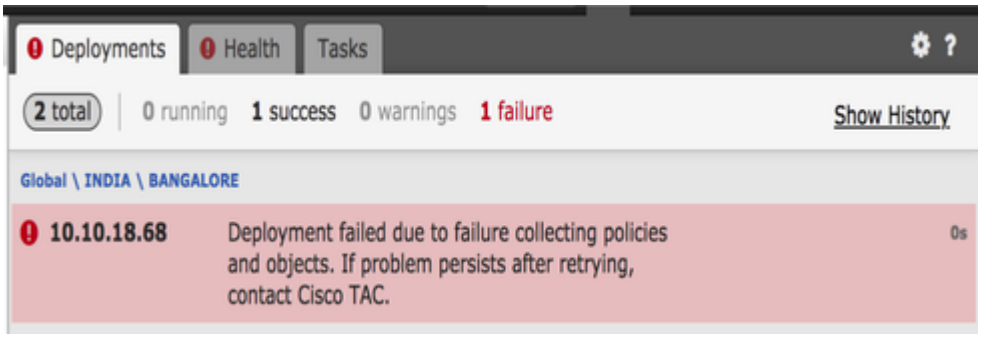
Common Issues/Error Messages

These are the errors/warnings shown in UI for FQDN and DNS server group object and DNS Settings:

Error/Warning	Scenario	Description
 Name contains invalid characters. Names must start with either alphabet or underscore and then either alphanumeric or special characters after. (-,_,+,.)	User configures wrong name.	User is informed of the allowed characters and max range.
 Invalid default domain value	User configures wrong domain name.	User is informed of the allowed characters and max range.
 No Interface Object has been selected for the DNS in platform setting ‘mzafeiro_Platform_Settings’. If proceeded, DNS domain-lookup is soon to happen on all interfaces	User does not select any interface for domain lookup. For a post-6.3 device	User is warned that the DNS server group CLI is soon to get applied to all interfaces.
 No Interface Object has been selected for the DNS in platform setting ‘mzafeiro_Platform_Settings’. If proceeded, no DNS server-group with ‘DNS’ is soon to be applied	User does not select any interface for domain lookup. For a 6.2.3 device	User is warned that the DNS server group CLI is not generated.

Deployment Failure

When an FQDN is used in policy other than AC Policy/Prefilter policy, this error can occur and is shown in the FMC UI:



Recommended Troubleshooting Steps

1) Open logfile: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) Check for validation message similar to:

“Invalid network(s) configured. Networks [NetworksContainingFQDN] configured on the device(s)[DeviceNames] refer to FQDN”



3) Suggested action:

Verify if one or more of the mentioned policies are already configured with a FQDN or group which contains a FQDN object(s) and re-try the deployment of the same after those object(s) are removed.

a) Identity Policy

b) Variable Sets that contain a FQDN-applied to AC Policy

No Activated FQDN

The system can show the next via the FTD CLI:

> show dns INFO: no activated FQDN

The DNS is not activated until an object with a defined fqdn is applied. After an object is applied, this is resolved.

Q&A

Q: Is Packet-tracer with FQDN a valid test to troubleshoot issues?
A: Yes, you can use fqdn option with packet-tracer.

Q: How often the FQDN rule updates the IP address of the server?
A: It depends on the TTL value of the DNS Response. Once the TTL value expires, the FQDN is resolved again with a new DNS query.
This also depends on the Poll Timer attribute defined in the DNS Server configuration. FQDN rule is resolved periodically when the Poll DNS timer has expired or when the TTL of the resolved IP entry has expired, whichever comes first.

Q: Does this work for round-robin DNS?
A: Round-robin DNS work seamlessly as this feature works on the FMC/FTD with the use of a DNS client and the round-robin DNS configuration is on the DNS server side.

Q: Is there a limitation for the low TTL DNS values?
A: If a DNS response comes with 0 TTL, the FTD device adds 60 seconds to it. In this case, the TTL value is minimum 60 seconds.

Q: So, by default, the FTD keeps the default value of 60 seconds?
A: The user can always override the TTL with Expire Entry Timer setting on DNS Server.

Q: How it interoperates with anycast DNS responses? For example, DNS servers can provide different IP addresses based on geolocation to requesters. Is it possible to request all IP addresses for a FQDN? Like the dig command on Unix?
A: Yes, if FQDN is able to resolve multiple IP addresses, all are be pushed to the device and the AC rule expands accordingly.

Q: Are there plans to include a preview option that shows the commands is pushed before any deployment change?
A: This is part of the **Preview config** option available via Flex config. Preview is already there, but it is hidden in Flex Config policy. There is a plan to move it out and make it generic.

Q: Which interface on the FTD is used to perform the DNS lookup?

A: It is configurable. When no interfaces are configured, all named interfaces on FTD are enabled for the DNS lookup.

Q: Does each managed NGFW perform its own DNS resolution and FQDN IP translation separately even when the same Access Policy is applied on all of them with the same FQDN object?
A: Yes.

Q: Can the DNS cache be cleared for FQDN ACLs to troubleshoot?
A: Yes, you can perform the **clear dns** and **clear dns-hosts cache** commands on the device.

Q: When exactly is the FQDN resolution is triggered?
A: FQDN resolution happens when the FQDN object is deployed in an AC policy.

Q: Is it possible to purge the cache only for a single site?
A: Yes. If you know the domain name or IP address then you can clear it, but there is no command as such per ACL perspective. For example, the **clear dns host agni.tejas.com** command is present to clear the cache on host by host basis with the keyword host as in **dns host agni.tejas.com**.

Q: Is it possible to use wildcards, like *.microsoft.com?
A: No. FQDN must begin and end with a digit or letter. Only letters, digits, and hyphens are allowed as internal characters.

Q: Is name resolution performed at AC compilation time and not at the time of the first or subsequent requests? If you hit low TTL (less than AC compilation time, fast-flux or something else), can some IP addresses be missed?
A: Name resolution happens as soon as the AC policy is deployed. As per the TTL time expiry, the renewal ensues.

Q: Are there plans to be able to process Microsoft Office 365 cloud IP addresses (XML) list?
A: This is not supported at this time.

Q: Is FQDN available in SSL Policy?
A: Not for now (software version 6.3.0). FQDN objects are only supported in source and destination network for AC policy only.

Q: Are there any historic logs that can provide information about resolved FQDNs? Like LINA syslogs, for example.
A: To troubleshoot the FQDN to a particular destination, you can use the **system support trace** command. The traces show the FQDN ID of the packet. You can compare the ID to troubleshoot. You can also enable Syslog messages 746015, 746016 to track the FQDN dns resolution activity.

Q: Does the device log FQDN in connections table with resolved IP?
A: To troubleshoot the FQDN to a particular destination, you can use the **system support trace** command, where the traces show the FQDN ID of the packet. You can compare the ID to troubleshoot. There are plans to have FQDN logs in the event viewer on FMC in the future.

Q: What are the shortcomings of FQDN rule feature?

A: The feature does not scale if the FQDN rule is used on a destination that changes IP address frequently (for example: internet servers that have TTL expiry of zero), workstations can end up having new IP addresses that no longer match with the FTD DNS cache. As a result, it does not match the ACP rule. By default, the FTD adds 1 minute on top of the received TTL expiry from the DNS response and cannot be set to zero. On these conditions, it is highly recommended to use the URL Filtering feature that is best suited for this use case.