firepower脅威対策（FMCマネージド）のFQDN機能について

内容

はじめに

このドキュメントでは、Firepower Management Center(FMC)とFirepower Threat Defense(FTD)に対するFQDN機能（v6.3.0以降）の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- ソフトウェアバージョン6.3.0が稼働するシスコFirepower脅威対策(FTD)仮想
- ソフトウェアバージョン6.3.0が稼働するFirepower Management Center Virtual(vFMC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、ソフトウェアバージョン6.3.0でFirepower Management Center(FMC)およびFirepower Threat Defense(FTD)に導入された完全修飾ドメイン名(FQDN)機能の設定について説明します。

この機能はCisco適応型セキュリティアプライアンス(ASA)に搭載されていますが、FTDの初期ソフトウェアリリースには搭載されていませんでした。

FQDNオブジェクトを設定する前に、次の条件が満たされていることを確認してください。

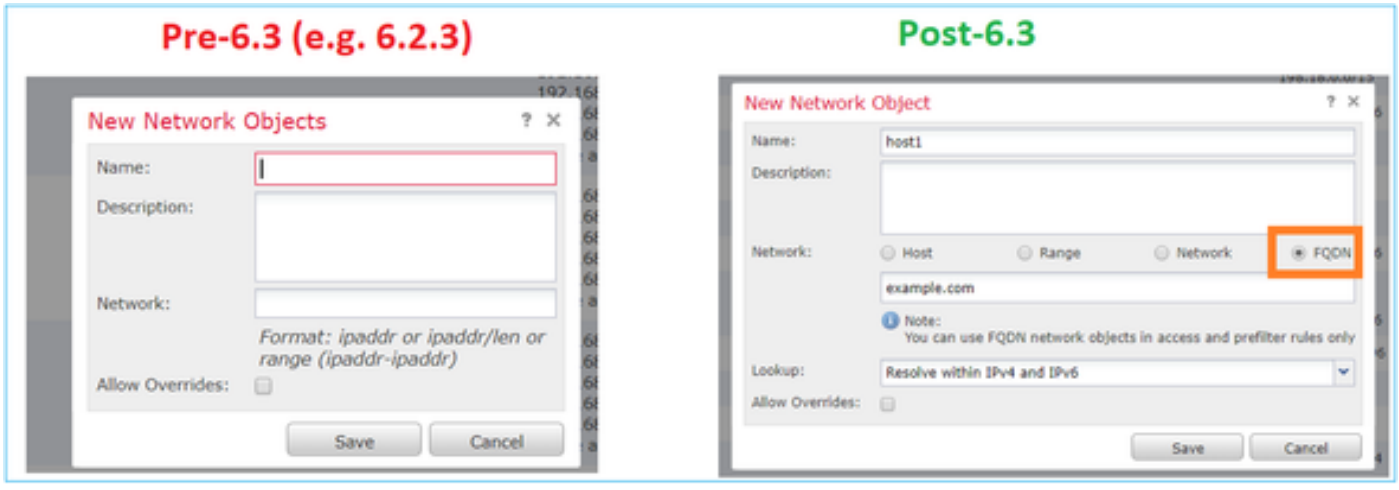
- firepower Management Centerは、バージョン6.3.0以降を実行する必要があります。物理または仮想
- firepower Threat Defense(FTD)は、バージョン6.3.0以降を実行する必要があります。物理または仮想

機能の概要

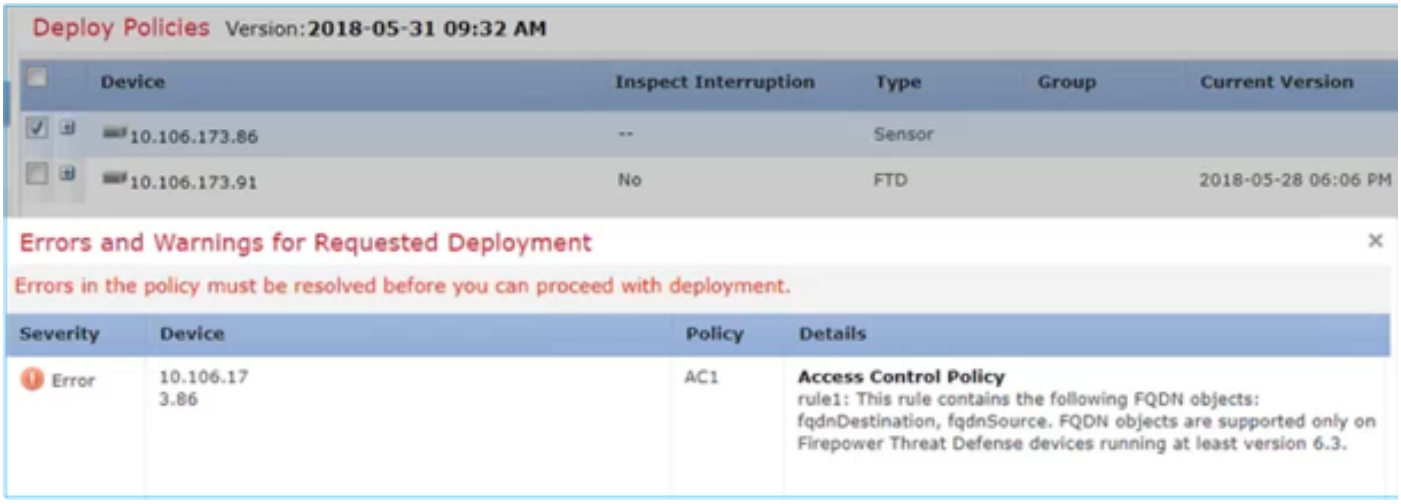
この機能は、FQDNをIPアドレスに解決し、アクセスコントロールルールまたはプレフィルタポリシーによって参照されるトラフィックをIPアドレスを使用してフィルタリングします。

6.3より前のバージョンはどうですか。

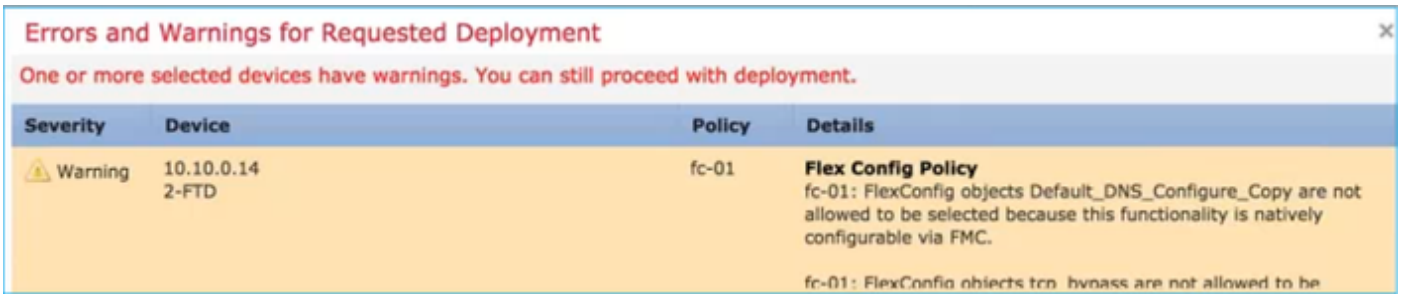
- 6.3.0より前のバージョンが稼働するFMCおよびFTDでは、FQDNオブジェクトを設定できません。



- FMCがバージョン6.3以降を実行しているが、FTDが6.3よりも前のバージョンを実行している場合、ポリシーの展開には次のエラーが表示されます。

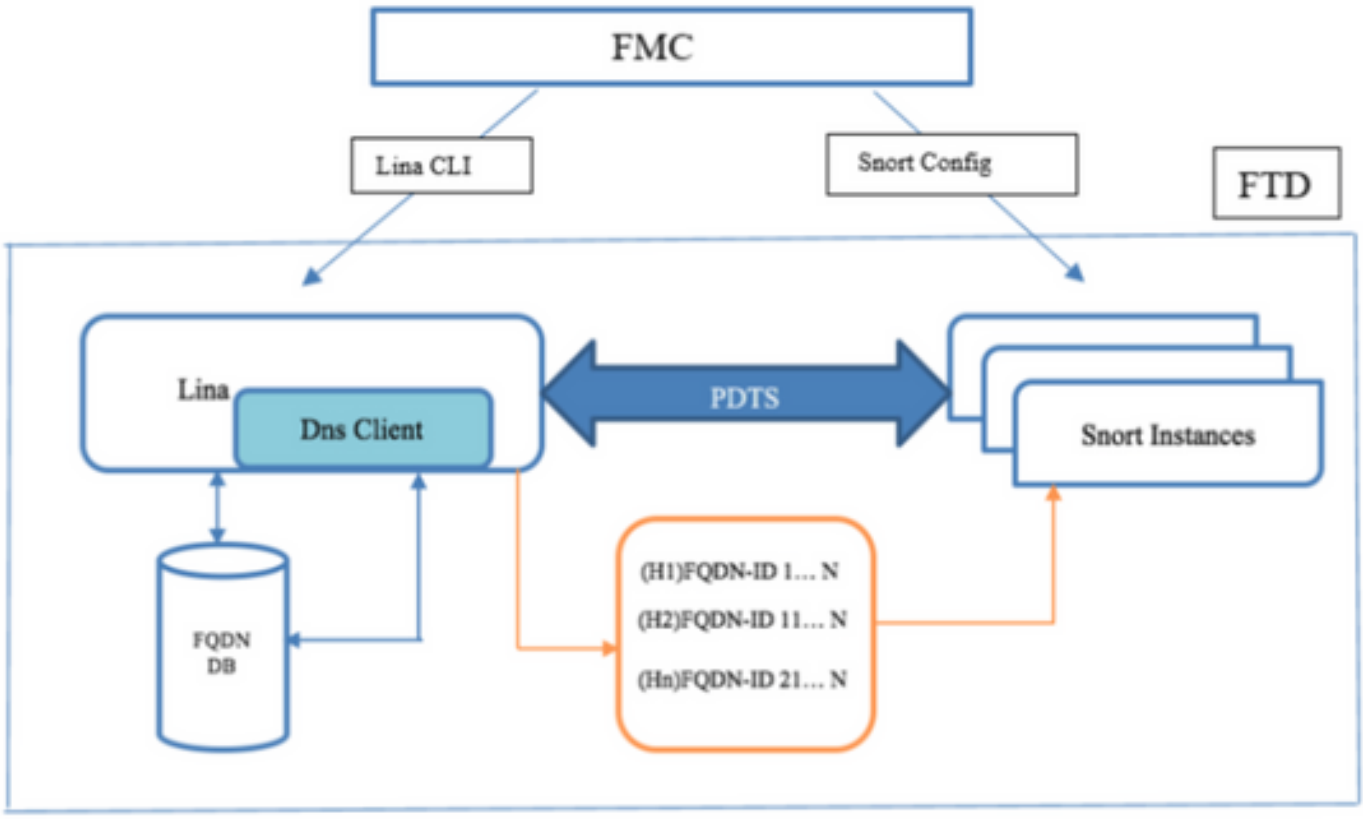


- また、FlexConfigでDNSオブジェクトを設定すると、次の警告が表示されます。



設定

ネットワーク図

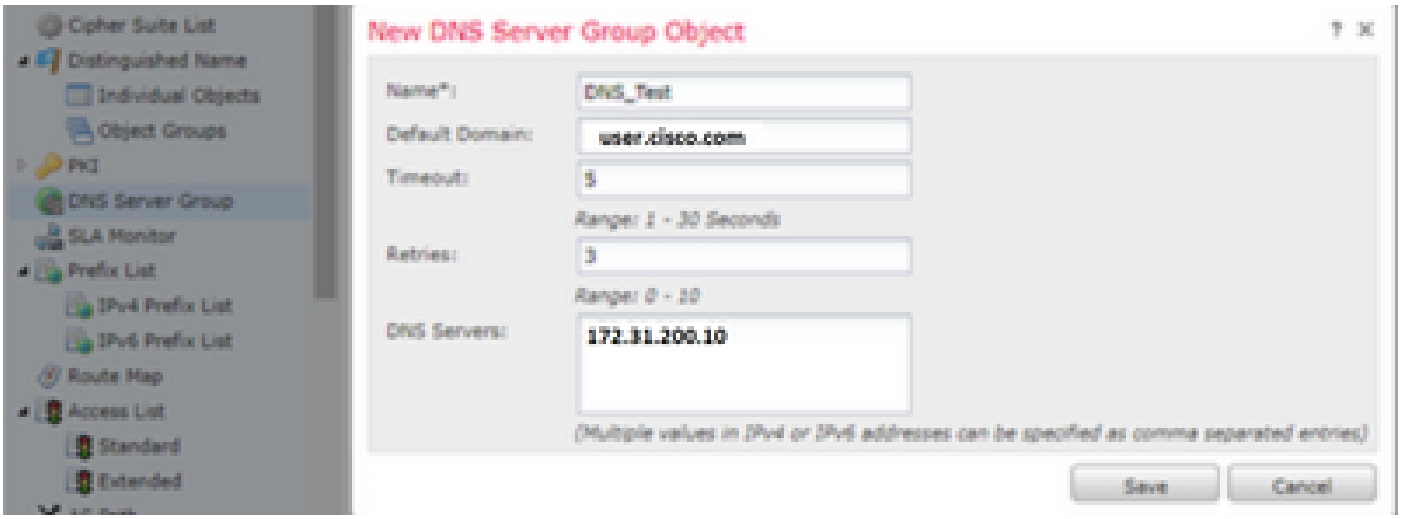


アーキテクチャ – 重要ポイント

- LINAでDNS解決（DNSからIP）が行われる
- LINAはマッピングをデータベースに格納します
- 接続ごとに、このマッピングはLINAからSnortに送信されます
- FQDNの解決は、ハイアベイラビリティまたはクラスタの設定に関係なく行われます

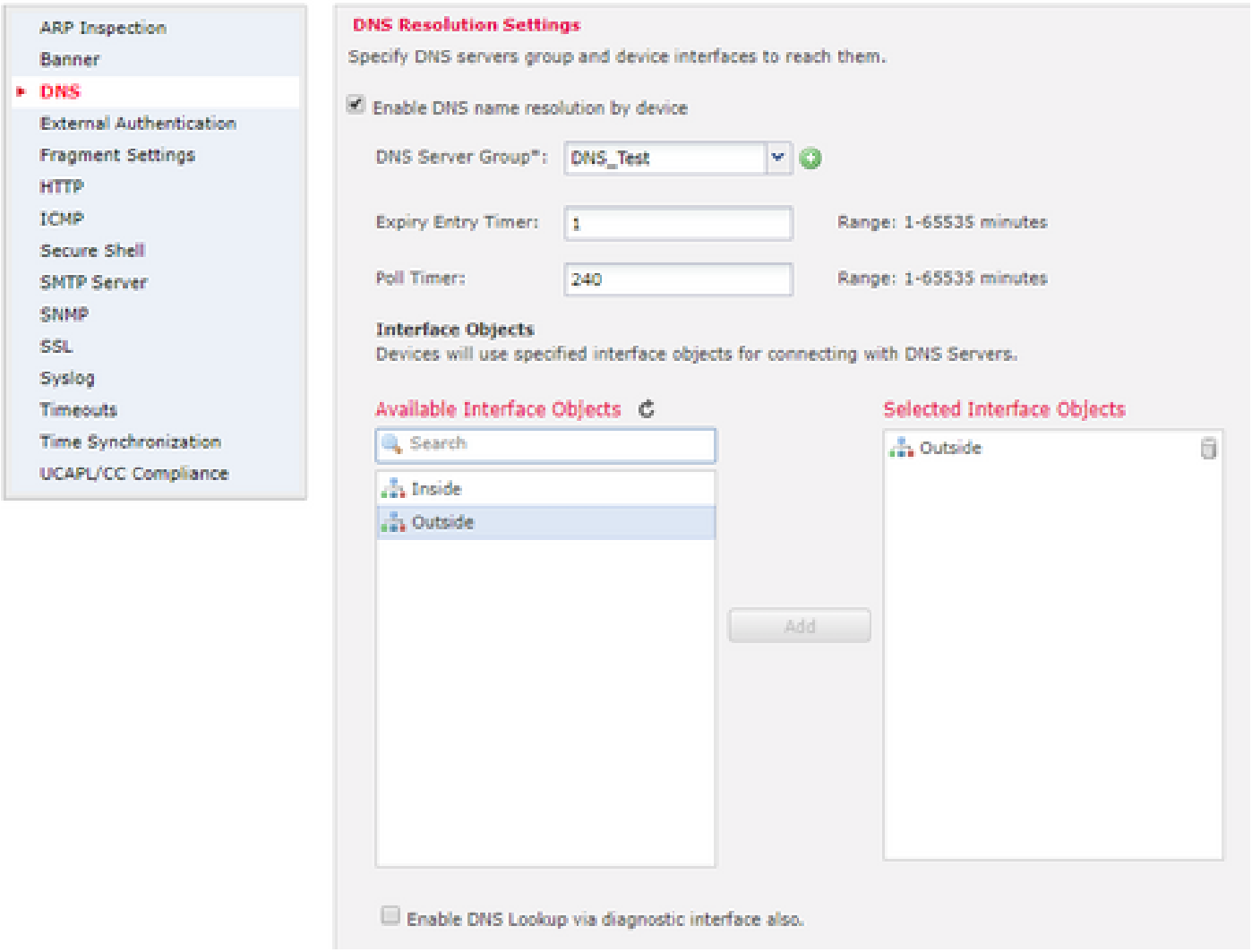
設定手順

ステップ 1：「DNSサーバグループオブジェクト」の設定



- DNSサーバーグループ名は63文字以内にする必要があります
- マルチドメイン展開では、オブジェクト名はドメイン階層内で一意である必要があります。現在のドメインで表示できないオブジェクトの名前と競合が識別される場合があります
- Default Domain（オプション）は、完全修飾されていないホスト名に追加するために使用されます
- デフォルトの再試行回数とタイムアウト値は事前に入力されています。
    - Retries：システムが応答を受信しないときに、DNSサーバのリストを再試行する回数 (0 ~ 10)。デフォルト値は 2 です。
    - Timeout：次のDNSサーバへの接続が試行されるまでの秒数（1 ~ 30秒）。デフォルト値は 2 秒です。システムがサーバのリストを再試行するたびに、このタイムアウトは2倍になります。
- このグループに属するDNSサーバを入力します。これは、カンマ区切り値としてIPv4またはIPv6のいずれかの形式にすることができます
- DNSサーバグループは、インターフェイスオブジェクトまたはプラットフォーム設定で設定されたオブジェクトによる解決に使用されます
- DNSサーバグループオブジェクトCRUD用のREST APIがサポートされています

ステップ 2：DNSの設定（プラットフォーム設定）



- （オプション）Expiry Entry TimerとPoll Timerの値を分単位で変更します。

expiry entry timerオプションは、解決済みFQDNのIPアドレスをDNSルックアップテーブルから削除する制限時間(TTL)を指定します。エントリを削除するにはテーブルを再コンパイルする必要があるため、削除を頻繁に行うとデバイスのプロセス負荷が増大する可能性があります。この設定により、TTLが実質的に拡張されます。

poll timerオプションは、ネットワークオブジェクトグループで定義されたFQDNを解決するためにデバイスがDNSサーバに照会するまでの時間の制限を指定します。FQDNは、ポーリングタイマーの期限が切れたか、解決されたIPエントリのTTLが切れたか、どちらか早い方のタイミングで定期的に解決されます。

- （オプション）使用可能なリストから必要なインターフェイスオブジェクトを選択し、それらを[選択したインターフェイスオブジェクト]リストに追加して、選択したインターフェイスからDNSサーバに到達できるようにします。

firepower Threat Defense(FTD)6.3.0デバイスでは、インターフェイスが選択されておらず、診断インターフェイスでDNSルックアップが無効になっている場合、診断インターフェイスを含むすべてのインターフェイスでDNS解決が行われます（コマンドdnsdomain-lookup anyが適用されます）。

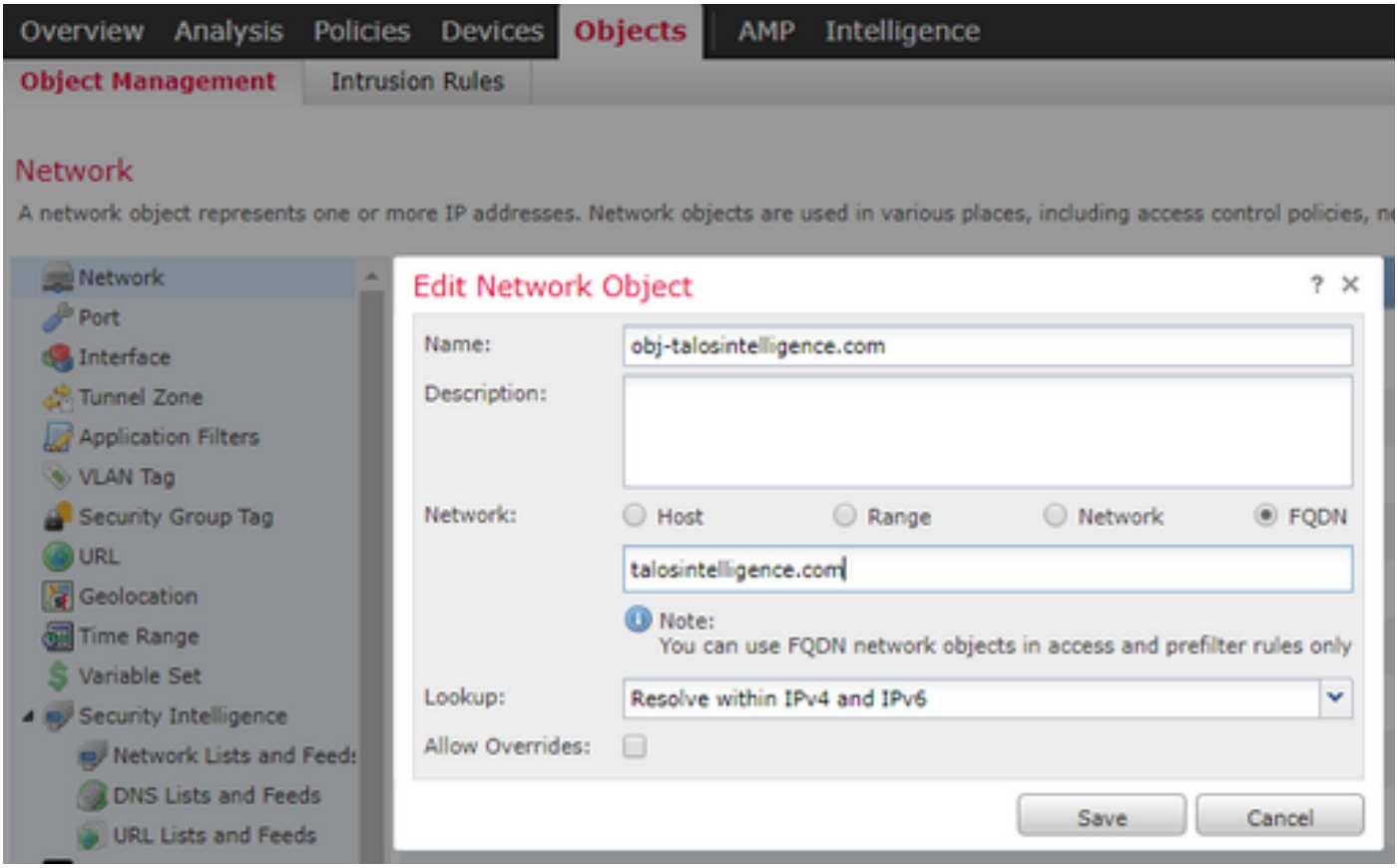
インターフェイスを指定せず、診断インターフェイスでDNSルックアップを有効にしない場合、FTDはデータルーティングテーブルを使用してインターフェイスを決定します。一致するものがない場合は、管理ルーティングテーブルが使用されます。

- （オプション）Enable DNS Lookup via the diagnostic interface alsoチェックボックスを選択します

有効にすると、Firepower Threat Defenseは選択されたデータインターフェイスと診断インターフェイスの両方を使用してDNS解決を行います。Devices > Device Management > edit device > Interfacesページで、診断インターフェイスのIPアドレスを必ず設定してください。

ステップ 3： オブジェクトネットワークFQDNの設定

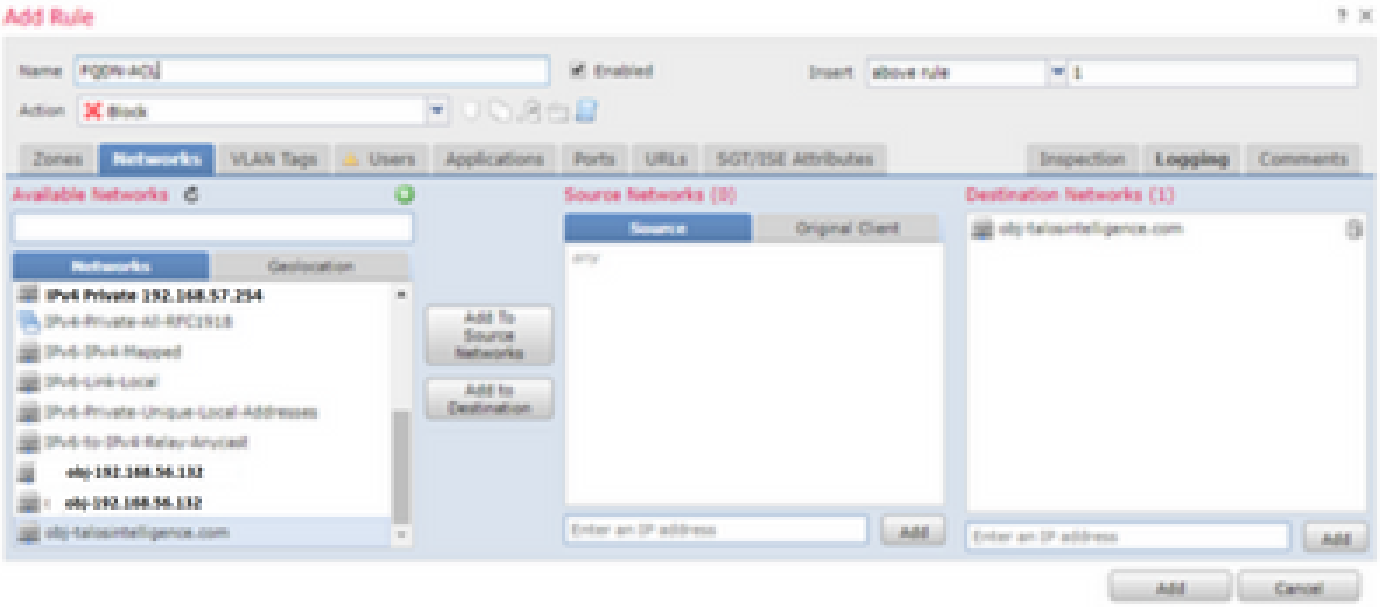
Objects > Object Managementに移動し、ネットワークオブジェクト内でFQDNオプションを選択します。

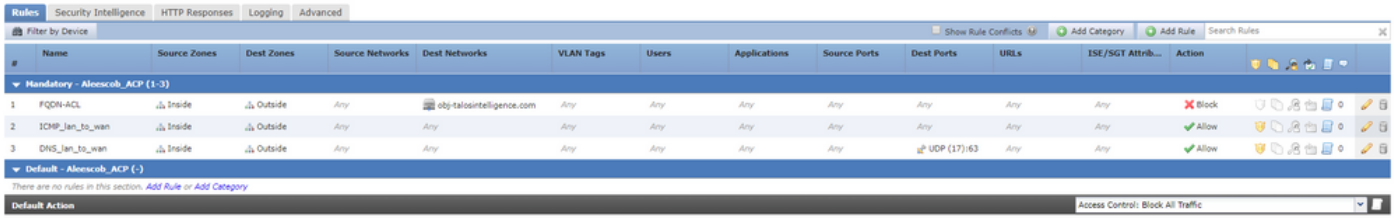


- ユーザがFQDNオブジェクトを作成すると、32ビットの一意のIDが生成されます
- このIDは、FMCからLINAとSnortの両方にプッシュされます
- LINAでは、このIDはオブジェクトに関連付けられます
- Snortでは、このIDは、そのオブジェクトを保持するアクセス制御規則に関連付けられます

ステップ 4：アクセスコントロールルールの作成

前のFQDNオブジェクトを使用してルールを作成し、ポリシーを展開します。





注：FQDN解決の最初のインスタンスは、FQDNオブジェクトがアクセスコントロールポリシーに展開されるときに発生します

確認

ここでは、設定が正常に動作していることを確認します。

- FQDNが展開される前のFTDの初期設定を次に示します。

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

- FQDNを展開した後の設定を次に示します。

```
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
```

- LINAでは、FQDNオブジェクトは次のように表示されます。

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

- すでに展開されている場合、FQDNアクセスリストはLINAで次のように表示されます。

```
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.com
```

- Snort(ngfw.rules)では次のように表示されます。

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

注：このシナリオでは、宛先にFQDNオブジェクトが使用されているため、dstfqdnとしてリストされます。

- show dnsコマンドとshow fqdnコマンドを確認すると、tallosintelligenceのIPの解決が開始されたことがわかります。

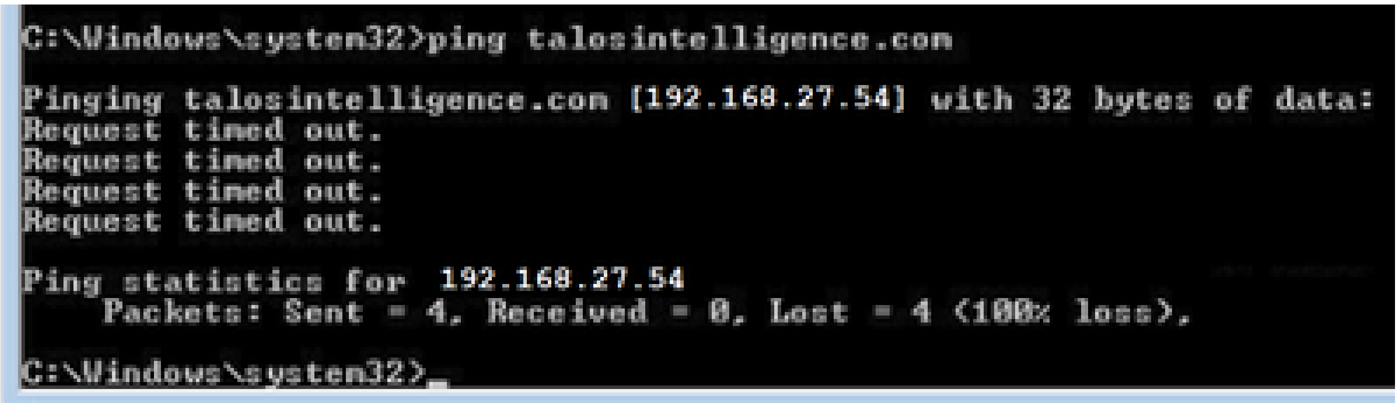
```
aleescob# show dns
Name: talosintelligence.com
  Address: 2001:DB8::6810:1b36                          TTL 00:05:43
  Address: 2001:DB8::6810:1c36                          TTL 00:05:43
  Address: 2001:DB8::6810:1d36                          TTL 00:05:43
  Address: 2001:DB8::6810:1a36                          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
```

- LINAでshow access-listにチェックマークを入れると、解決とヒットカウントごとにエントリが拡張されていることがわかります。

```
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
```

- 図に示すように、アクセスリストに一致するFQDNがあるため、talosintelligence.comへのpingは失敗します。ICMPパケットがFTDによってブロックされているため、DNS解決は機能しています。



- 以前に送信されたICMPパケットのLINAからのヒットカウント：

```
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要求がキャプチャされ、入力インターフェイスでドロップされたことが示されます。

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 > 172.31.4.16 1 icmp：エコー要求3: 18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp：エコー応答4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp：要求 5: 18:04:13.462149 172.31.4 61 > 192.168.56.132 icmp：エコー応答6: 18:04:14.308425 192.168.56.132 > 172.31.4.161 icmp：エコー要求7: 18:04:14.475424 172.31.4.161> 192.168.56.132 icmp：応答8: 8:04:15.306823 192.168.56.132 > 172.31.4.161 icmp：エコー要求 9: 18:04:15.463339 172.31.4.161 > 192.168.56.132 icmp：エコー応答10: 18:04:25.713662 192.168.56.13 > 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 1 3: 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 1 18:04:35.711556 192.168.56.132 > 192.168.27.54 icmp：エコー要求176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp：エコー要求

- トレースは次のICMPパケットのいずれかを探します。

```
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
```

- アクセスコントロールルールのアクションがAllowの場合の出力例は、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
```

- FQDNがプレフィルタ(Fastpath)の一部として展開される場合、ngfw.rulesでは次のように表示されます。

```
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.
```

- トレースされたパケットのLINAの観点から：

```
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:
```

トラブルシュート

1. FMCからの設定

- ポリシーとDNSサーバ設定が正しく設定されていることを確認します。
- 導入が正常に行われたことを確認する

2. FTDでのチェックの導入

- show dnsおよびshow access-listを実行して、FQDNが解決され、ACルールが展開されているかどうかを確認します
- show run object networkを実行し、オブジェクトに関連付けられたIDを書き留めます（たとえば、ソースに対してX）。
- show fqdn id Xを実行して、FQDNが送信元IPに正しく解決されているかどうかを確認します
- ngfw.rulesファイルに、FQDN ID Xを送信元とするACルールが含まれているかどうかを確認します
- システムサポートfirewall-engine-debugを実行し、Snortの判定を確認します。

FMCのトラブルシューティングファイルの収集

必要なすべてのログは、FMCのトラブルシューティングから収集されます。FMCからすべての重要なログを収集するには、FMC GUIからトラブルシューティングを実行します。それ以外の場合は、FMC Linuxプロンプトからsf_troubleshoot.plを実行します。問題が見つかった場合は、レポートとともにFMCのトラブルシューティングをCisco Technical Assistance Center(TAC)に送信してください。

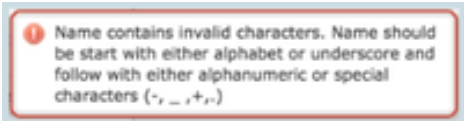
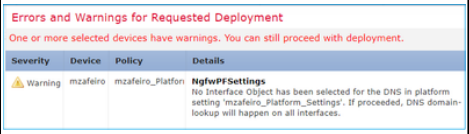
FMCログ

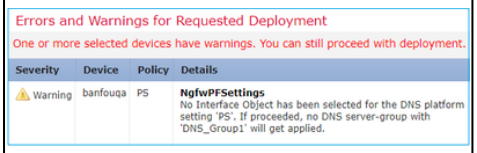
ログファイルの名前/場所	目的
/opt/CSCOpx/MDC/log/operation/vmssshareddsvcs.log	すべてのAPIコール
/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log	すべてのAPIコール
/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log	CLI生成ログ
/opt/CSCOpx/MDC/tomcat/logs/stdout.log	Tomcatログ
/var/log/mojo.log	Mojoログ

/var/log/CSMAgent.log	CSMとDC間のRESTコール
/var/log/action_queue.log	DCのアクションキューログ

一般的な問題とエラーメッセージ

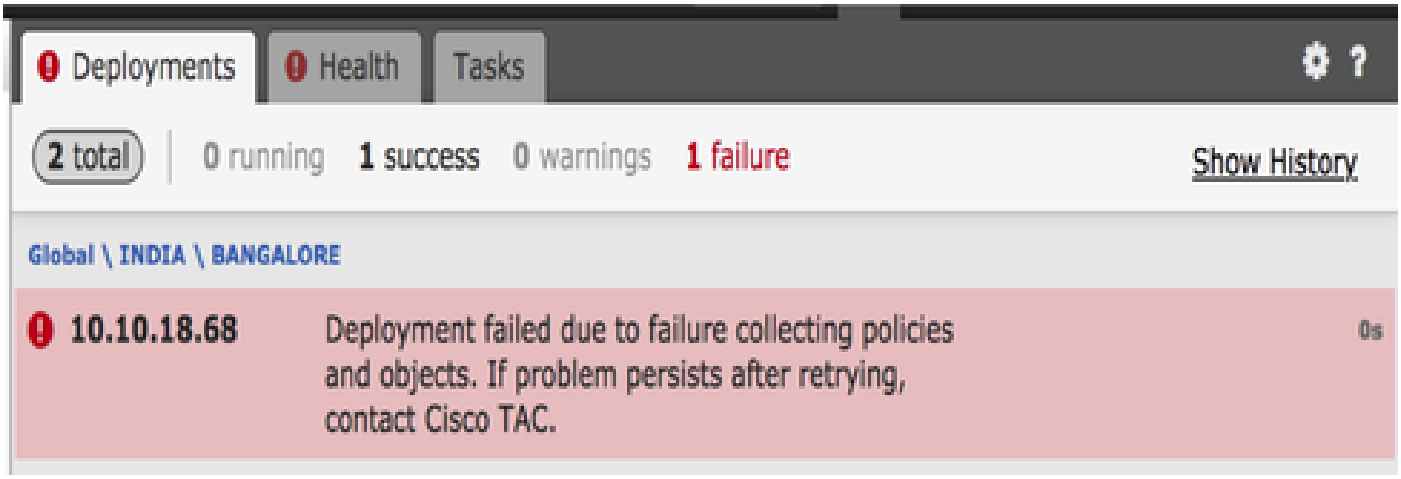
FQDNとDNSサーバグループオブジェクト、およびDNS設定のUIに表示されるエラーと警告は次のとおりです。

エラー/警告	シナリオ	説明
 名前に無効な文字が含まれています。名前は、アルファベットまたはアンダースコアで始まり、その後に英数字または特殊文字で始まる必要があります。(-,_,+,.)	User 誤った名前を設定する	ユーザに許可されたURLが通知されます 文字と最大範囲。
 既定のドメイン値が無効です	ユーザが誤ったドメイン名を設定している	ユーザには、許可される文字と最大範囲が通知されます。
 プラットフォーム設定'mzafeiro_Platform_Settings'でDNSのインターフェイスオブジェクトが選択されていません。処理が進むと、すべてのインターフェイスでDNSドメインルックアップが間もなく実行されます	ユーザがドメインルックアップ用のインターフェイスを選択しない 6.3以降のデバイス	ユーザに対して、DNS サーバグループCLIは間もなく適用されます すべてのインターフェイスに適用されます。

 プラットフォーム設定'mzafeiro_Platform_Settings'でDNSのインターフェイスオブジェクトが選択されていません。続行すると、「DNS」を含むDNSサーバグループはまもなく適用されなくなります	ユーザがドメインルックアップ用のインターフェイスを選択しない 6.2.3デバイス用	ユーザに警告が表示される DNSが サーバグループのCLIが 生成されます。

導入の失敗

ACポリシー/プレフィルタポリシー以外のポリシーでFQDNを使用すると、次のエラーが発生し、FMC UIに表示されます。



推奨されるトラブルシューティング手順

1)ログファイルを開きます：/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2)次のような検証メッセージを確認します。

“無効なネットワークが設定されています。デバイス[DeviceNames]に構成されているネットワーク[NetworksContainingFQDN]はFQDNを参照しています。

3)推奨されるアクション：

以下に示す1つ以上のポリシーが、FQDNオブジェクトを含むFQDNまたはグループで既に構成されているかどうかを確認し、それらのオブジェクトを削除した後に同じポリシーの展開を再試行してください。

a)アイデンティティポリシー

b) ACポリシーに適用されるFQDNを含む変数セット

アクティブ化されたFQDNがありません

システムはFTD CLIを使用して次のメッセージを表示できます。

> show dns INFO：アクティブ化されたFQDNがありません

定義されたfqdnを持つオブジェクトが適用されるまで、DNSはアクティブ化されません。オブジェクトが適用されると、この問題は解決されます。

Q&A

Q:FQDNを使用したパケットトレーサは、問題をトラブルシューティングするための有効なテストですか。
A：はい。fqdnオプションをpacket-tracerで使用できます。

Q: FQDNルールによってサーバのIPアドレスが更新される頻度はどのくらいですか。
A:DNS応答のTTL値によって異なります。TTL値が期限切れになると、FQDNは新しいDNSクエリで再度解決されます。
これは、DNSサーバの設定で定義されているPoll Timer属性によっても異なります。FQDNルールは、Poll DNSタイマーが時間切れになった場合、または解決されたIPエントリのTTLが時間切れになった場合に、どちらか早い方で定期的に解決されます。

Q：これはラウンドロビンDNSで機能しますか。
A：この機能はDNSクライアントを使用するFMC/FTDで動作し、ラウンドロビンDNS設定はDNSサーバ側にあるため、ラウンドロビンDNSはシームレスに動作します。

Q：低いTTL DNS値に制限はありますか。
A:DNS応答のTTLが0の場合、FTDデバイスは60秒を追加します。この場合、TTL値は最小60秒です。

Q:FTDはデフォルトで60秒のデフォルト値を維持しているのですか。
A：ユーザは、DNSサーバのExpire Entry Timer設定でTTLを常に上書きできます。

Q：エニーキャストDNS応答とどのように相互運用されるのですか。たとえば、DNSサーバは要求者に対して位置情報に基づいて異なるIPアドレスを提供できます。FQDNのすべてのIPアドレスを要求できますか。UNIXのdigコマンドと同様ですか。
A：はい。FQDNが複数のIPアドレスを解決できる場合、すべてのアドレスがデバイスにプッシュされ、それに応じてACルールが拡張されます。

Q：導入が変更される前にコマンドがプッシュされたことを示すプレビューオプションを含める計画はありますか。
A：これは、Flex Configで使用できるPreview configオプションの一部です。プレビューは既に存在しますが、Flex Configポリシーでは非表示になっています。今後は移行して汎用化する予定です。

Q: DNSルックアップの実行に使用されるのは、FTDのどのインターフェイスですか。
A：設定可能です。インターフェイスが設定されていない場合、FTDのすべての名前付きインターフェイスでDNSルックアップが有効になります。

Q：管理対象の各NGFWは、同じFQDNオブジェクトを持つすべてのNGFWに同じアクセスポリシーが適用されている場合でも、独自のDNS解決とFQDN IP変換を個別に実行しますか。
A：はい。

Q:FQDN ACLのトラブルシューティングのためにDNSキャッシュをクリアできますか。
A：はい。デバイスでclear dnsコマンドとclear dns-hosts cacheコマンドを実行できます。

Q:FQDN解決がトリガーされるのはいつですか。
A:FQDN解決は、FQDNオブジェクトがACポリシーに導入されるときに行われます。

Q：単一サイトのキャッシュだけを消去することはできますか。
A：はい。ドメイン名またはIPアドレスがわかっている場合はクリアできますが、ACLの観点からそのようなコマンドはありません。たとえば、clear dns host agni.tejas.comコマンドは、dns host agni.tejas.comのようにキーワードhostを使用して、ホストごとにキャッシュをクリアするために存在します。

Q: *.microsoft.comのようにワイルドカードを使用できますか。
A：いいえ。FQDNは数字または文字で始まり、終わる必要があります。内部文字として使用できるのは、文字、数字、ハイフンのみです。

Q：名前解決は、最初の要求または後続の要求の時点ではなく、ACのコンパイル時に実行されるのですか。TTLが低い（ACコンパイル時間、ファストフラックスなどの値より短い）場合、IPアドレスの一部が失われますか。
A：名前解決は、ACポリシーが展開されるとすぐに行われます。TTL時間の経過に従って、更新が行われます。

Q: Microsoft Office 365クラウドのIPアドレス(XML)リストを処理できる計画はありますか。
A：現時点ではサポートされていません。

Q:FQDNはSSLポリシーで使用できますか。
A：現時点ではサポートされていません（ソフトウェアバージョン6.3.0）。FQDNオブジェクトは、ACポリシーの送信元および宛先ネットワークでのみサポートされます。

Q：解決されたFQDNに関する情報を提供できる履歴ログはありますか。たとえば、LINA syslogなどです。
A：特定の宛先に対するFQDNのトラブルシューティングを行うには、system support traceコマンドを使用できます。トレースは、パケットのFQDN IDを示します。IDを比較してトラブルシューティングを行うことができます。Syslogメッセージ746015および746016を有効にして、FQDN dns解決アクティビティを追跡することもできます。

Q：デバイスは、解決済みIPを使用して接続テーブルにFQDNを記録しますか。
A：特定の宛先に対するFQDNのトラブルシューティングを行うには、system support traceコマンドを使用します。このコマンドのトレースには、パケットのFQDN IDが表示されます。IDを比較してトラブルシューティングを行うことができます。将来的には、FMCのイベントビューアにFQDNログを作成する予定です。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。