firepower 위협 방어(FMC-Managed)의 FQDN 기능 이해

목차

소개

이 문서에서는 FMC(Firepower Management Center) 및 FTD(Firepower Threat Defense)에 대한 FQDN 기능(v6.3.0 기준) 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 관리 센터

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.3.0을 실행하는 Cisco FTD(Firepower Threat Defense) 가상
- 소프트웨어 버전 6.3.0을 실행하는 vFMC(firepower 관리 센터 가상)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 소프트웨어 버전 6.3.0에서 FMC(Firepower Management Center) 및 FTD(Firepower Threat Defense)에 도입한 FQDN(Fully Qualified Domain Name) 기능의 컨피그레이션에 대해 설명합니다.

이 기능은 Cisco ASA(Adaptive Security Appliance)에 있지만 FTD의 초기 소프트웨어 릴리스에는 없었습니다.

FQDN 개체를 구성하기 전에 다음 조건을 충족해야 합니다.

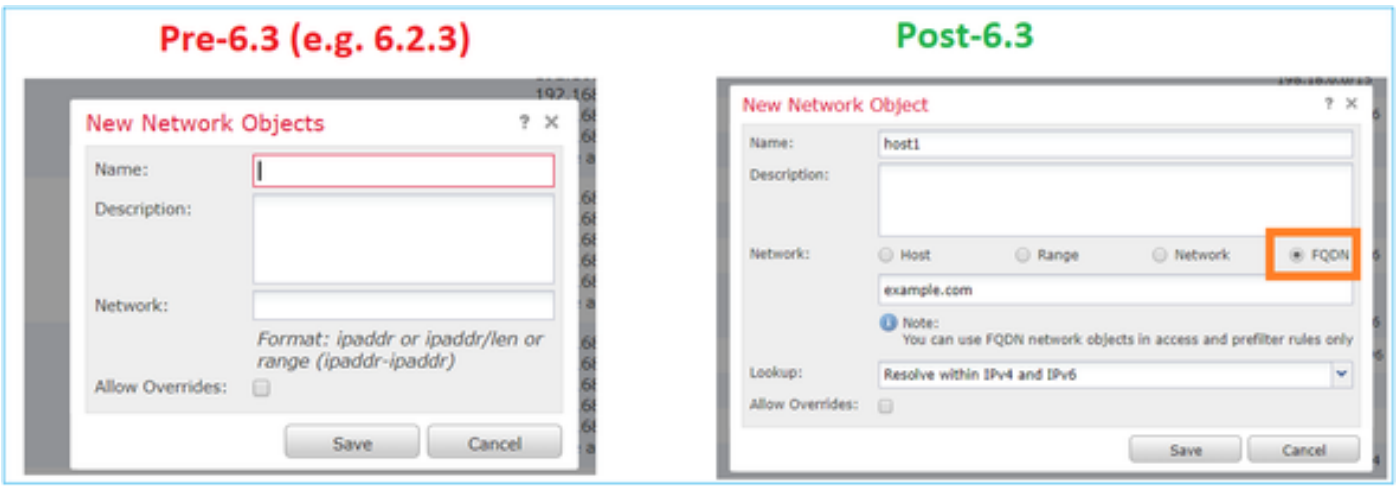
- firepower Management Center는 버전 6.3.0 이상을 실행해야 합니다. 물리적 또는 가상 환경일 수 있음
- firepower Threat Defense는 버전 6.3.0 이상을 실행해야 합니다. 물리적 또는 가상 환경일 수 있음

기능 개요

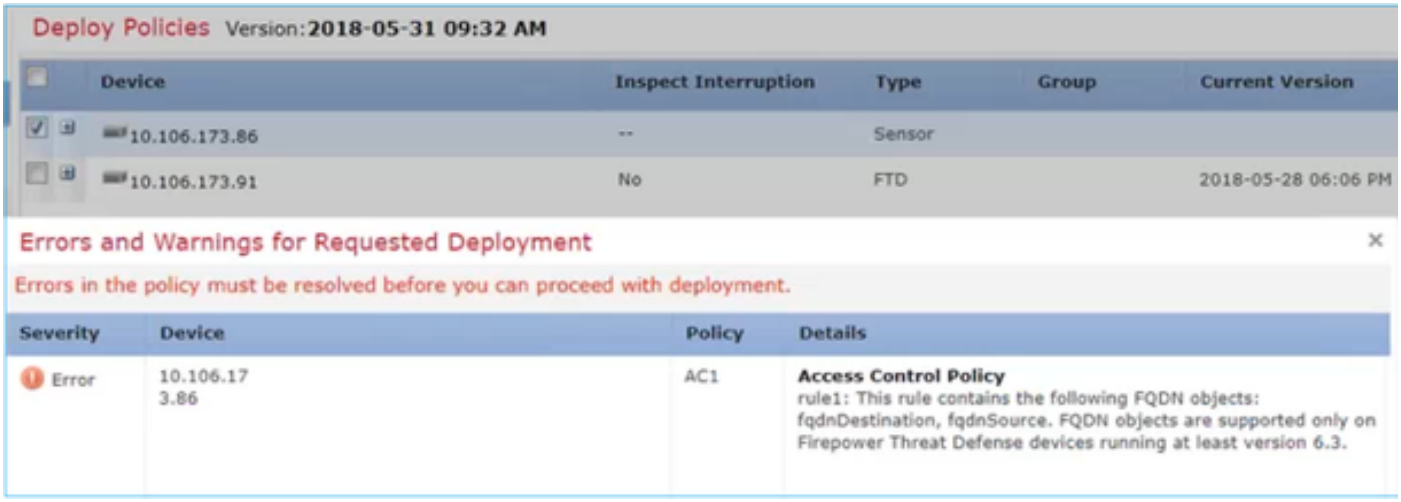
이 기능은 FQDN을 IP 주소로 확인하고 액세스 제어 규칙 또는 사전 필터 정책에서 참조하는 경우 후자를 사용하여 트래픽을 필터링합니다.

6.3 이전은요?

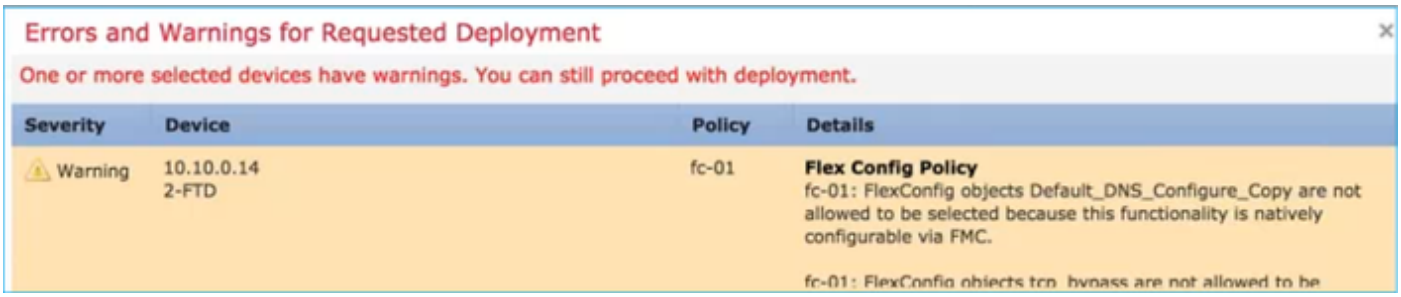
- 6.3.0 이전 버전을 실행하는 FMC 및 FTD는 FQDN 개체를 구성할 수 없습니다.



- FMC에서 버전 6.3 이상을 실행하지만 FTD에서 버전 6.3 이전 버전을 실행하는 경우 정책 구축에서 다음 오류가 표시됩니다.

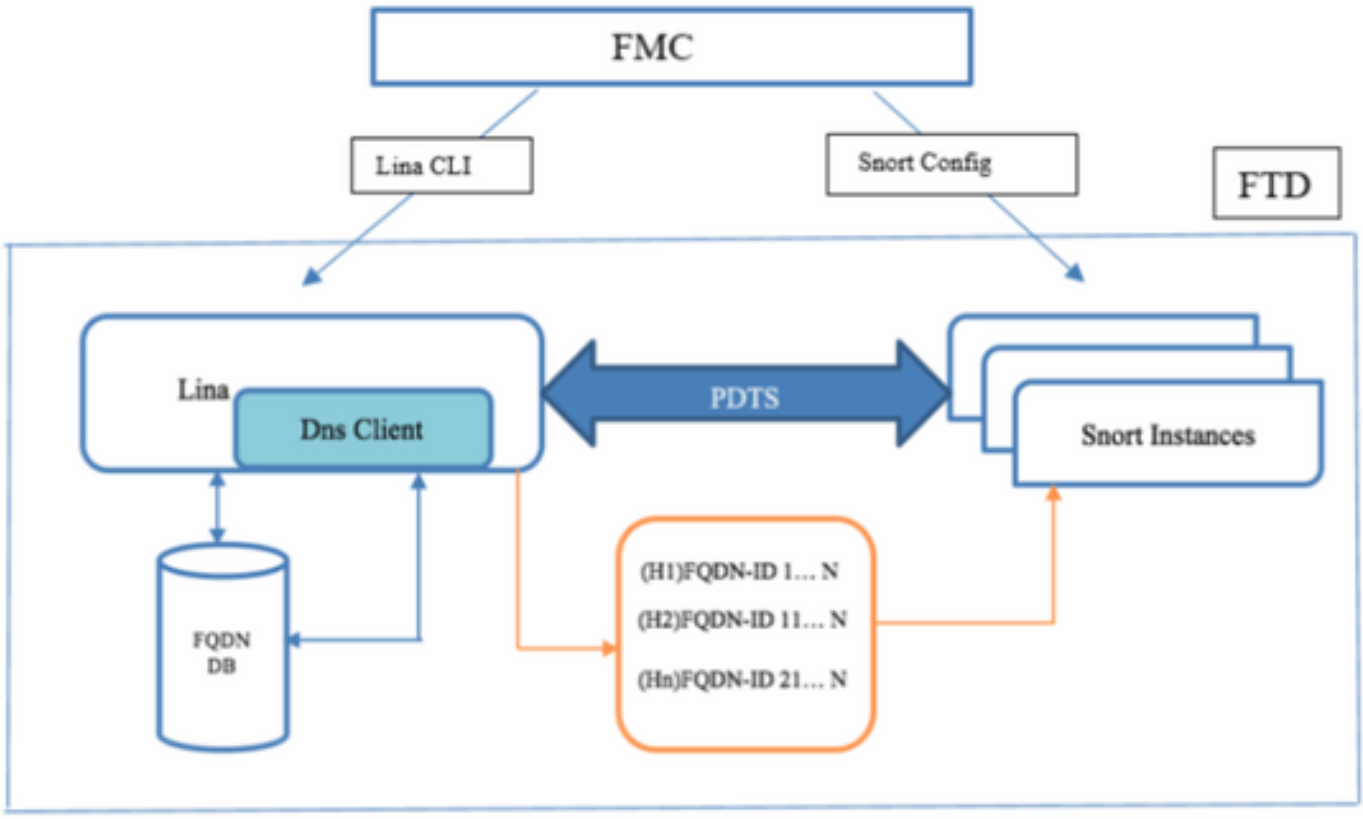


- 또한 FlexConfig를 통해 DNS 객체를 구성할 경우 다음 경고가 표시됩니다.



구성

네트워크 다이어그램

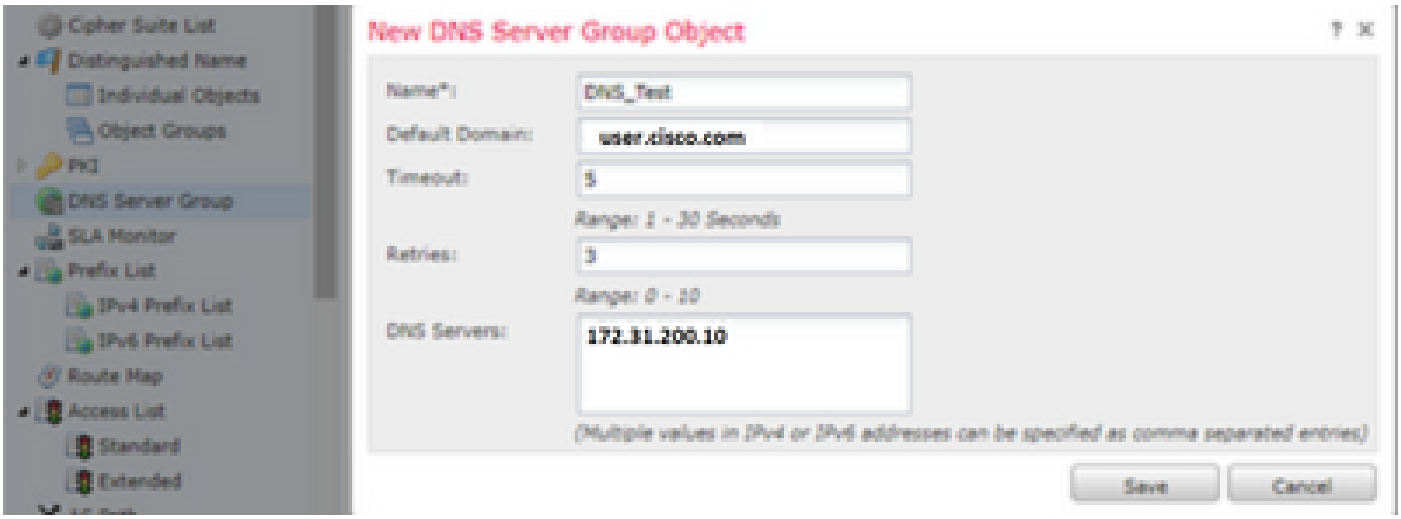


아키텍처 - 중요 포인트

- DNS 확인(DNS-IP)은 LINA에서 이루어짐
- LINA는 데이터베이스에 매핑을 저장합니다
- 연결별로 이 매핑은 LINA에서 Snort로 전송됩니다
- FQDN 확인은 고가용성 또는 클러스터 컨피그레이션과 독립적으로 수행됩니다

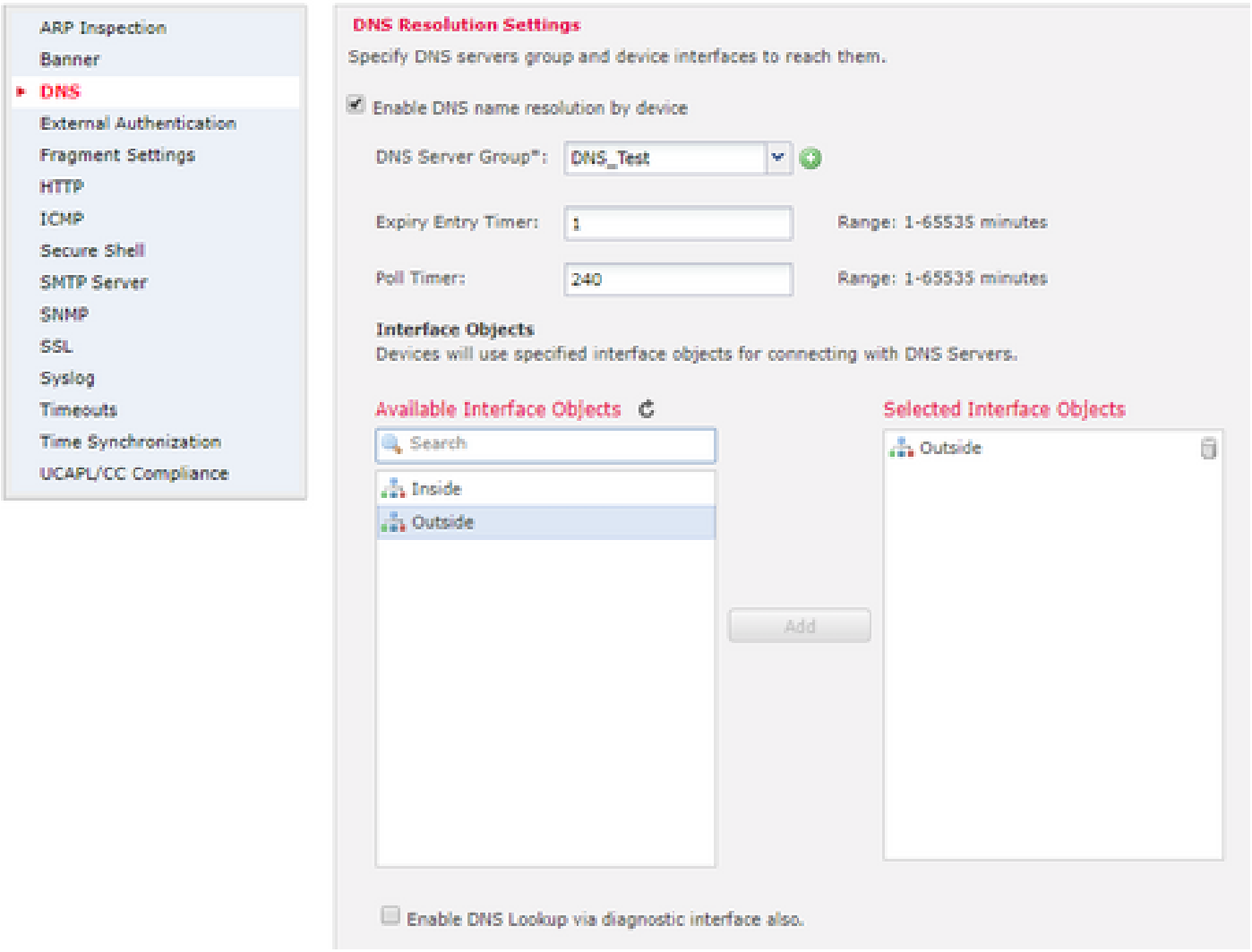
컨피그레이션 단계

1단계. "DNS 서버 그룹 개체" 구성



- DNS 서버 그룹 이름은 63자를 초과할 수 없습니다.
- 다중 도메인 구축에서 개체 이름은 도메인 계층 구조 내에서 고유해야 합니다. 시스템은 현재 도메인에서 볼 수 없는 객체의 이름과 충돌을 식별할 수 있습니다
- 기본 도메인(선택 사항)은 정규화되지 않은 호스트 이름에 추가하는 데 사용됩니다
- 기본 Retries(재시도 횟수) 및 Timeout(시간 초과) 값은 미리 채워집니다.
    - Retries(재시도 횟수) - 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수(0~10)입니다. 기본값은 2입니다.
    - Timeout(시간 제한) - 다른 서버가 다음 DNS 서버로 시도하기 전 1~30초 사이의 시간(초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 제한은 두 배가 됩니다.
- 이 그룹에 속할 DNS 서버를 입력합니다. 쉼표로 구분된 값으로 IPv4 또는 IPv6 형식을 사용할 수 있습니다
- DNS 서버 그룹은 Platform Settings(플랫폼 설정)에서 구성된 인터페이스 개체를 사용하여 확인하는 데 사용됩니다
- DNS 서버 그룹 개체 CRUD에 대한 REST API가 지원됩니다.

2단계. DNS(플랫폼 설정) 구성



- (선택 사항) 만료 항목 타이머 및 폴링 타이머 값을 분 단위로 수정합니다.

만료 항목 타이머 옵션은 TTL(Time-to-live)이 만료된 후 DNS 조회 테이블에서 확인된 FQDN의 IP 주소를 제거하는 시간 제한을 지정합니다. 항목을 제거하려면 테이블을 다시 컴파일해야 하므로 자주 제거하면 디바이스의 프로세스 로드가 증가할 수 있습니다. 이 설정은 TTL을 가상으로 확장합니다.

poll timer 옵션은 디바이스가 네트워크 객체 그룹에 정의된 FQDN을 확인하기 위해 DNS 서버를 쿼리할 때까지의 시간 제한을 지정합니다. FQDN은 폴링 타이머가 만료된 경우 또는 확인된 IP 항목의 TTL이 만료된 경우 중 먼저 발생하는 경우에 주기적으로 확인됩니다.

- (선택 사항) 사용 가능한 목록에서 필수 인터페이스 객체를 선택하고 이를 Selected Interface Objects 목록에 추가한 다음 선택한 인터페이스를 통해 DNS 서버에 연결할 수 있는지 확인합니다.

firepower Threat Defense 6.3.0 디바이스의 경우 인터페이스가 선택되지 않았고 진단 인터페이스가 DNS 조회에 대해 비활성화되어 있으면 진단 인터페이스가 포함된 모든 인터페이스를 통해 DNS 확인이 수행됩니다(dnsdomain-lookup any 명령이 적용됨).

인터페이스를 지정하지 않고 진단 인터페이스에서 DNS 조회를 활성화하지 않으면 FTD는 데이터 라우팅 테이블을 사용하여 인터페이스를 결정합니다. 일치하는 항목이 없으면 관리 라우팅 테이블

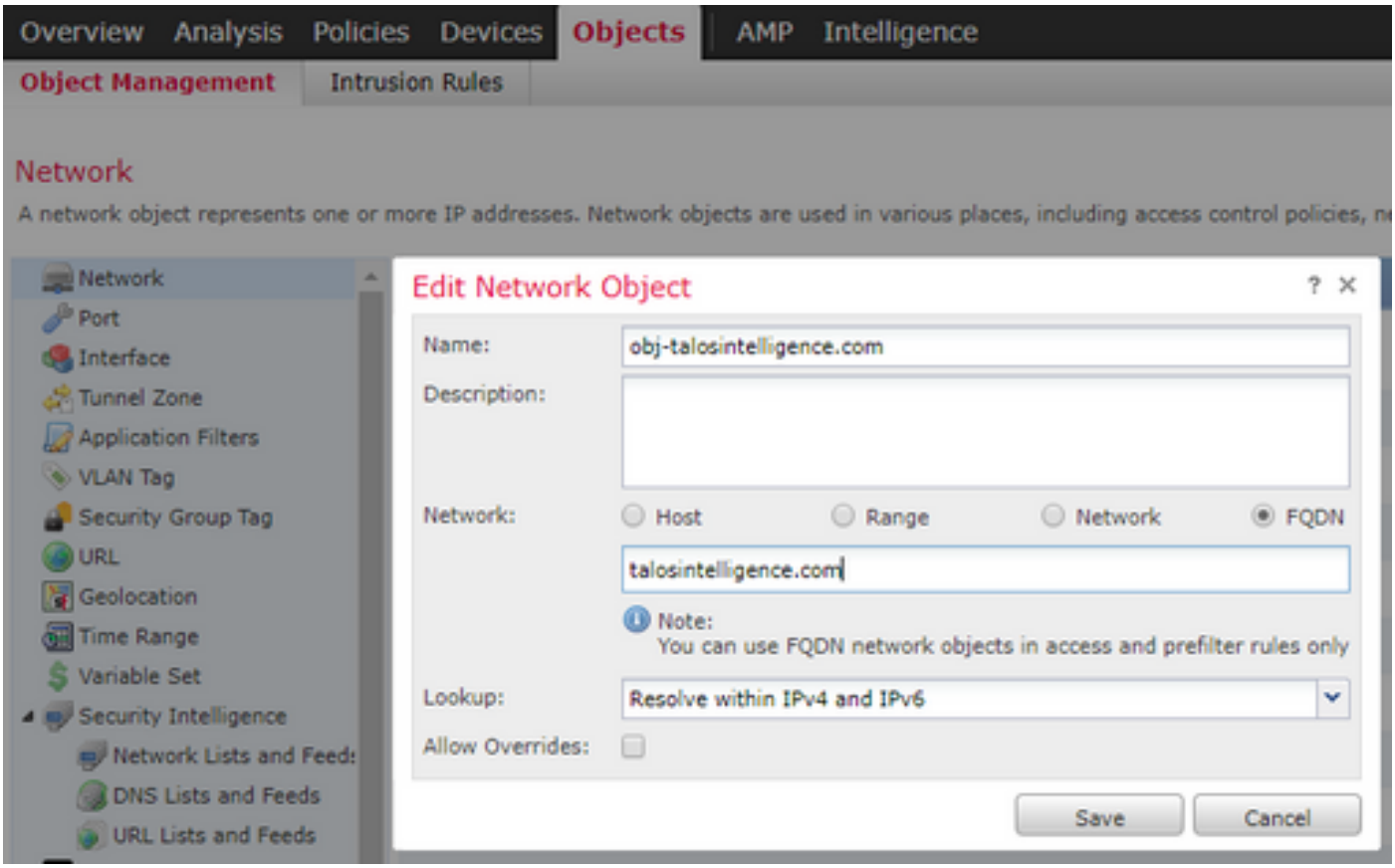
을 사용합니다.

- (선택 사항) Enable DNS Lookup via the diagnostic interface also 확인란을 선택합니다

활성화된 경우 Firepower Threat Defense는 선택한 데이터 인터페이스와 진단 인터페이스를 모두 사용하여 DNS 확인을 수행합니다. Devices > Device Management > edit device > Interfaces 페이지에서 진단 인터페이스에 대한 IP 주소를 구성해야 합니다.

3단계. 개체 네트워크 FQDN 구성

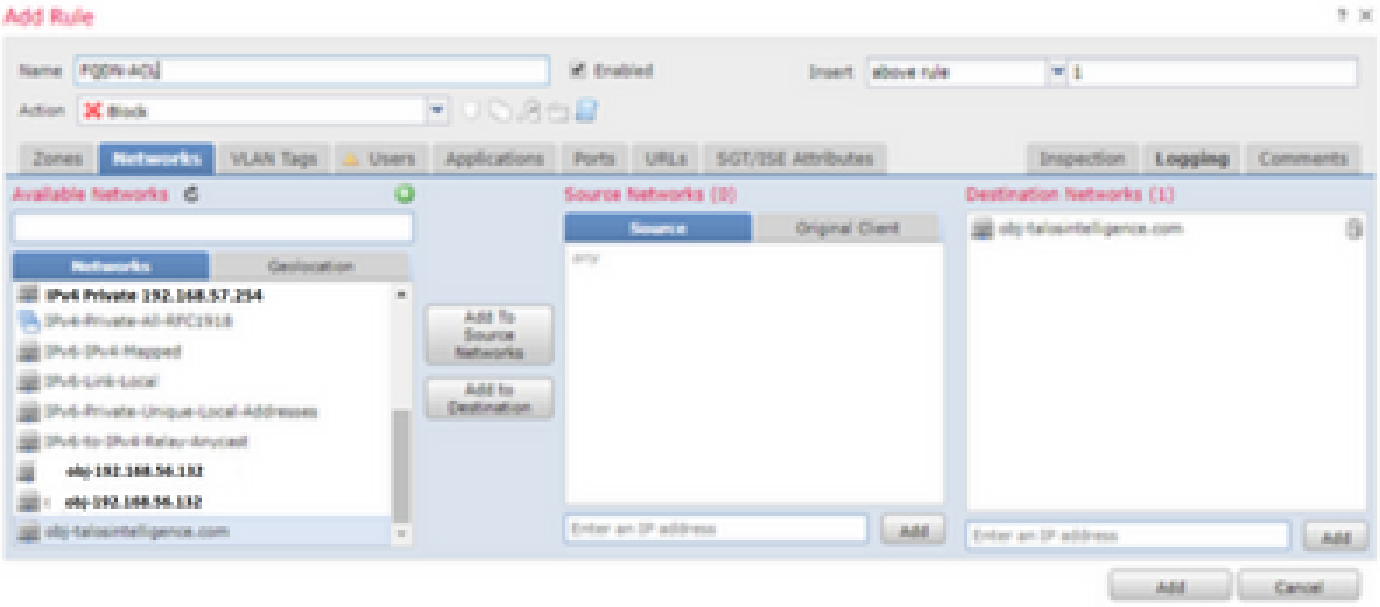
Objects(개체) > Object Management(개체 관리)로 이동하고 네트워크 개체 내에서 FQDN 옵션을 지정합니다.

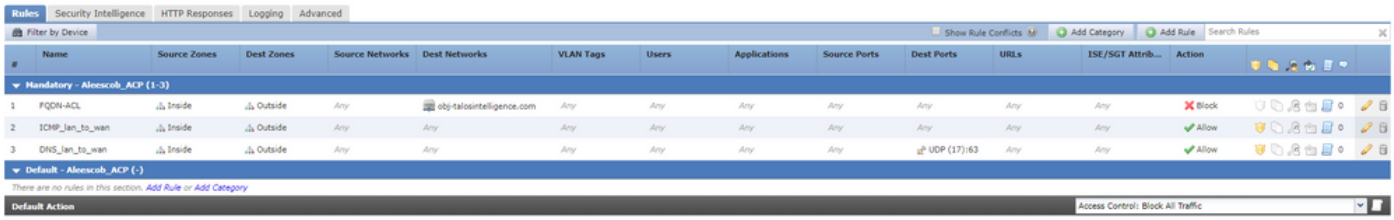


- 사용자가 FQDN 개체를 만들 때 32비트 고유 ID가 생성됩니다
- 이 ID는 FMC에서 LINA 및 Snort 모두로 푸시됩니다.
- LINA에서 이 ID는 개체와 연결되어 있습니다.
- snort에서 이 ID는 해당 객체를 보유하는 액세스 제어 규칙과 연결됩니다

4단계. 액세스 제어 규칙 생성

이전 FQDN 개체로 규칙을 생성하고 정책을 구축합니다.





참고: FQDN 확인의 첫 번째 인스턴스는 FQDN 개체가 액세스 제어 정책에 배포될 때 발생합니다

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- 다음은 FQDN을 구축하기 전의 FTD 초기 컨피그레이션입니다.

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

- FQDN 구축 이후의 컨피그레이션입니다.

```
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
```

- 다음은 LINA에서 FQDN 개체가 표시되는 방식입니다.

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

- 이미 구축된 FQDN access-list는 다음과 같이 LINA에서 표시됩니다.

```
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
```

- Snort(ngfw.rules)에서는 다음과 같은 모습을 보여줍니다.

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

참고: 이 시나리오에서 FQDN 객체는 대상에 사용되었으므로 dstfqdn으로 나열됩니다.

- show dns 및 show fqdn 명령을 선택한 경우 이 기능이 talosintelligence용 IP를 확인하기 시작했음을 알 수 있습니다.

```
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
```

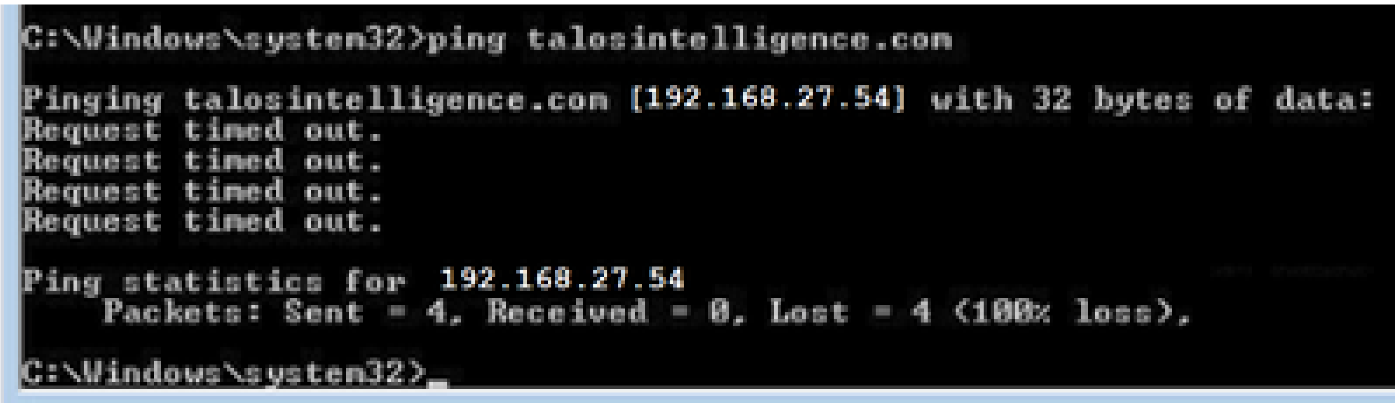
```
aleescob# show fqdn
FQDN IP Table:
ip = 2001:DB8::6810:1b36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

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:DI
```

- LINA에서 show access-list를 선택하면 각 해상도 및 적중 횟수에 대해 확장된 항목을 확인할 수 있습니다.

```
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
```

- 이미지에 표시된 대로 액세스 목록에 FQDN에 대한 일치가 있으므로 talosintelligence.com에 대한 ping이 실패합니다. ICMP 패킷이 FTD에 의해 차단되었으므로 DNS 확인이 작동했습니다.



- 이전에 보낸 ICMP 패킷에 대한 LINA의 히트 수:

```
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 요청이 캡처되고 인그레스 인터페이스에서 삭제된 것으로 표시됩니다.

alescob# 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 > 192.1 68.56.132 icmp: 에코 응답 4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp: 에코 요청 5: 18:04:13.462149 172.31.4.161 > 192.168.56.132 icmp: 에코 응답 6: 18:04:14.308425 192.168.56.132 > 172.31.4.161 icmp: 에코 요청 7: 1:18:40:14.475424 172.31.4.161> 192.168.56.132 icmp: 에코 응답 8: 18:04:15.306823 192.168.56.132 > 172.31.4.161 icmp: 에코 요청 9: 18:04:15.463339 172.31.4.161 > 192.168.56.132 icmp: 에코 응답 10: 18:04:25.7136622.168.56.1 32 > 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 192.16 8.27.54 icmp: echo request alescob# sho cap asp | 192.168.27.54 162: 18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp: 에코 요청 165: 18:04:30.704355 192.168.56.132 > 192.168.27.54 icmp: 에코 요청 168: 18:04:35.711556 192.168.56.132 > 192.16 .27.54 icmp: echo request 176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp: echo request

- 추적이 다음 ICMP 패킷 중 하나를 찾는 방법입니다.

```
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
```

- 액세스 제어 규칙의 작업이 Allow인 경우, 이는 시스템 지원 firewall-engine-debug 출력의 예입니다

```
> 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
```

- FQDN이 Prefilter(Fastpath)의 일부로 구축된 경우 ngfw.rules에서는 다음과 같은 방식으로 표시됩니다.

```
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.
```

- 추적된 패킷을 포함하는 LINA 관점에서:

```
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:
```

문제 해결

1. FMC에서 구성

- 정책 및 DNS 서버 설정이 올바르게 구성되었는지 확인
- 배포가 성공적인지 확인합니다.

2. FTD에 대한 확인 구축

- show dns 및 show access-list를 실행하여 FQDN이 확인되고 AC 규칙이 확장되었는지 확인합니다.
- show run object network를 실행하고 객체와 연결된 ID를 기록해 둡니다(예: 소스의 경우 X).
- show fqdn id X를 실행하여 FQDN이 소스 IP로 올바르게 확인되었는지 확인합니다.
- ngfw.rules 파일에 FQDN ID가 X인 AC 규칙이 있는지 확인합니다.
- 시스템 지원 firewall-engine-debug를 실행하고 Snort 판정 확인

FMC 문제 해결 파일 수집

필요한 모든 로그는 FMC 트러블슈팅에서 수집됩니다. FMC에서 모든 중요한 로그를 수집하려면 FMC GUI에서 Troubleshoot(문제 해결)을 실행합니다. 그렇지 않은 경우 FMC Linux 프롬프트에서 sf_troubleshoot.pl을 실행합니다. 문제가 발견되면 보고서와 함께 FMC 트러블슈팅을 Cisco TAC(Technical Assistance Center)에 제출하십시오.

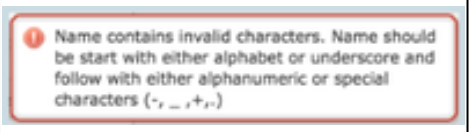
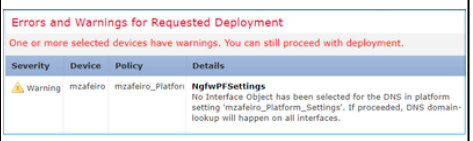
FMC 로그

로그 파일 이름/위치	목적
/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log	모든 API 호출
/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log	모든 API 호출
/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log	CLI 생성 로그
/opt/CSCOpx/MDC/tomcat/logs/stdout.log	Tomcat 로그
/var/log/mojo.log	Mojo 로그
/var/log/CSMAgent.log	CSM과 DC 간의 REST 통화

/var/log/action_queue.log	DC의 작업 큐 로그

일반적인 문제/오류 메시지

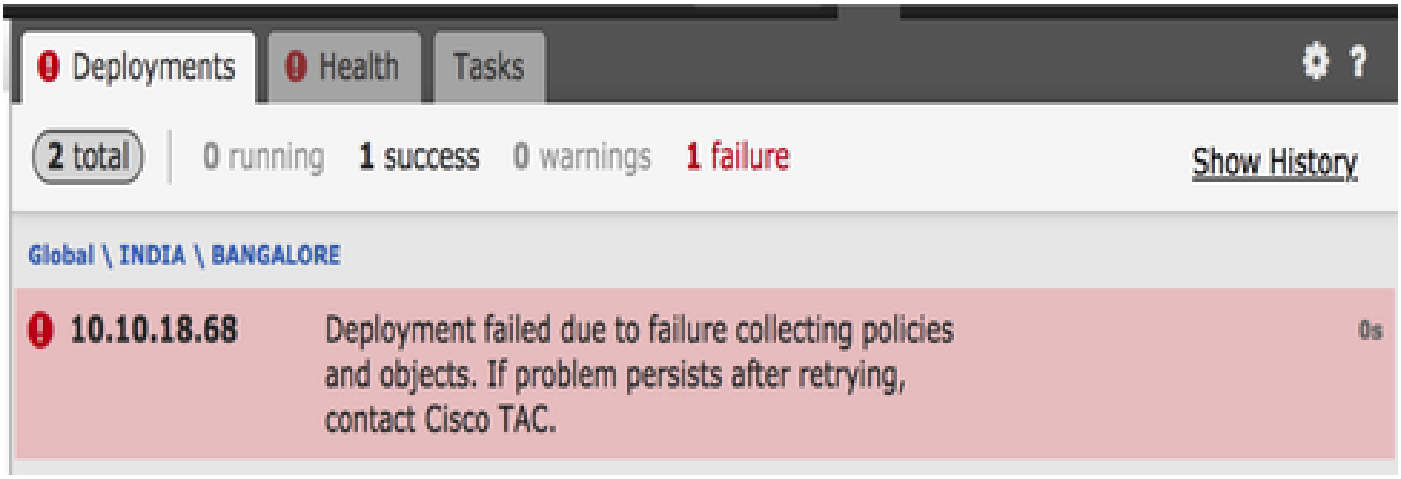
다음은 FQDN 및 DNS 서버 그룹 개체, DNS 설정에 대한 UI에 표시되는 오류/경고입니다.

오류/경고	시나리오	설명
 이름에 잘못된 문자가 있습니다. 이름은 알파벳 또는 밑줄로 시작하고 그 뒤에 영숫자 또는 특수 문자로 시작해야 합니다. (-,_,+,.)	사용자 잘못된 이름을 구성합니다.	사용자에게 허용된 알림 문자 및 최대 범위입니다.
 잘못된 기본 도메인 값	사용자가 잘못된 도메인 이름을 구성함	사용자에게 허용되는 문자 및 최대 범위가 표시됩니다.
 플랫폼 설정 'mzafeiro_Platform_Settings'에서 DNS에 대해 선택된 인터페이스 개체가 없습니다. 계속하면 모든 인터페이스에서 DNS 도메인 조회가 곧 수행됩니다	사용자가 도메인 조회를 위해 어떤 인터페이스도 선택하지 않음 6.3 이후 디바이스의 경우	사용자에게 DNS에 대한 경고 서버 그룹 CLI가 곧 적용될 예정입니다. 모든 인터페이스에 적용됩니다.
 플랫폼 설정 'mzafeiro_Platform_Settings'에서 DNS에 대해 선택된 인터페이	사용자가 도메인 조회를 위해 어떤 인터페이스도 선택하지 않음 6.2.3 장치의 경우	사용자에게 경고 DNS가 서버 그룹 CLI가 생성되었습니다.

스 개체가 없습니다. 진행하면 'DNS'가 있는 DNS 서버 그룹을 곧 적용할 수 없습니다.		

구축 실패

FQDN이 AC 정책/사전 필터 정책 이외의 정책에서 사용되는 경우 이 오류가 발생하여 FMC UI에 표시될 수 있습니다.



권장 문제 해결 단계

1) 로그 파일 열기: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) 다음과 유사한 검증 메시지를 확인합니다.

"잘못된 네트워크가 구성되었습니다. 디바이스에 구성된 네트워크 [NetworksContainingFQDN][DeviceNames]는 FQDN을 참조합니다."

3) 권장 조치:

FQDN 개체가 포함된 FQDN 또는 그룹으로 아래 언급한 정책 중 하나 이상이 이미 구성되어 있는지 확인하고 해당 개체를 제거한 후 동일한 정책을 다시 구축하십시오.

a) ID 정책

b) AC 정책에 적용된 FQDN을 포함하는 변수 집합

활성화된 FQDN 없음

시스템은 FTD CLI를 통해 다음을 표시할 수 있습니다.

> show dns INFO: 활성화된 FQDN 없음

DNS는 정의된 fqdn의 개체가 적용될 때까지 활성화되지 않습니다. 객체가 적용되면 이 문제가 해결됩니다.

질문과 대답

Q: FQDN이 있는 Packet-tracer는 문제 해결을 위한 유효한 테스트입니까?
A: 예. packet-tracer와 함께 fqdn 옵션을 사용할 수 있습니다.

Q: FQDN 규칙이 서버의 IP 주소를 업데이트하는 빈도는 얼마입니까?
A: DNS 응답의 TTL 값에 따라 달라집니다. TTL 값이 만료되면 FQDN이 새 DNS 쿼리로 다시 확인됩니다.
또한 DNS 서버 컨피그레이션에 정의된 Poll Timer 특성에도 따라 달라집니다. FQDN 규칙은 폴 DNS 타이머가 만료되거나 확인된 IP 항목의 TTL이 만료될 때(둘 중 먼저 오는 경우) 주기적으로 확인됩니다.

Q: 라운드 로빈 DNS에 적용됩니까?
A: 이 기능은 DNS 클라이언트를 사용하는 FMC/FTD에서 작동하며 라운드 로빈 DNS 컨피그레이션은 DNS 서버 측에 있으므로 라운드 로빈 DNS는 원활하게 작동합니다.

Q: 낮은 TTL DNS 값에 대한 제한이 있습니까?
A: DNS 응답에 TTL이 0이면 FTD 디바이스는 60초를 추가합니다. 이 경우 TTL 값은 최소 60초입니다.

Q: 기본적으로 FTD는 기본값을 60초로 유지합니까?
A: 사용자는 항상 DNS 서버의 Expire Entry Timer 설정으로 TTL을 재정의할 수 있습니다.

Q: 애니캐스트 DNS 응답과 어떻게 상호 운용됩니까? 예를 들어, DNS 서버는 지리적 위치에 따라 다른 IP 주소를 요청자에게 제공할 수 있습니다. FQDN에 대한 모든 IP 주소를 요청할 수 있습니까? 유닉스의 dig 명령처럼?
A: 예. FQDN에서 여러 IP 주소를 확인할 수 있는 경우 모두 디바이스로 푸시되며 AC 규칙이 그에 따라 확장됩니다.

Q: 구축 변경 전에 명령이 푸시됨을 보여주는 미리보기 옵션을 포함할 계획입니까?
A: Flex Config를 통해 사용 가능한 Preview 컨피그레이션 옵션의 일부입니다. 미리 보기는 이미 있지만 Flex Config 정책에 숨겨져 있습니다. 그것을 밖으로 옮기고 일반화하려는 계획이 있다.

Q: FTD에서 어떤 인터페이스를 사용하여 DNS 조회를 수행합니까?

A: 구성할 수 있습니다. 인터페이스가 구성되지 않은 경우 FTD의 모든 명명된 인터페이스가 DNS 조회를 위해 활성화됩니다.

Q: 관리되는 각 NGFW는 동일한 FQDN 개체를 사용하여 모든 NGFW에 동일한 액세스 정책이 적용되는 경우에도 자체 DNS 확인 및 FQDN IP 변환을 별도로 수행합니까?
A: 네.

Q: 트러블슈팅을 위해 FQDN ACL에 대한 DNS 캐시를 지울 수 있습니까?
A: 예. 디바이스에서 clear dns 및 clear dns-hosts cache 명령을 수행할 수 있습니다.

Q: 정확히 언제 FQDN 확인이 트리거됩니까?
A: FQDN 객체는 AC 정책에서 구축될 때 확인됩니다.

Q: 단일 사이트에 대해서만 캐시를 삭제할 수 있습니까?
A: 네. 도메인 이름 또는 IP 주소를 알고 있는 경우 이를 지울 수 있지만 ACL 관점에 따라 이와 같은 명령은 없습니다. 예를 들어 clear dns host agni.tejas.com 명령은 dns host agni.tejas.com에서와 같이 host 키워드를 사용하여 호스트별로 캐시를 지웁니다.

Q: *.microsoft.com과 같은 와일드카드를 사용할 수 있습니까?
A: 아니요. FQDN은 숫자 또는 문자로 시작하고 끝나야 합니다. 문자, 숫자 및 하이픈만 내부 문자로 허용됩니다.

Q: 이름 확인은 첫 번째 또는 후속 요청 시점이 아니라 AC 컴파일 시점에 수행됩니까? TTL이 낮으면(AC 컴파일 시간 미만, Fast-Flux 등) 일부 IP 주소를 놓칠 수 있습니까?
A: AC 정책이 구축되는 즉시 이름 확인이 이루어집니다. TTL 시간 만료에 따라 갱신이 계속됩니다.

Q: Microsoft Office 365 XML(클라우드 IP 주소) 목록을 처리할 수 있도록 계획되어 있습니까?
A: 현재는 지원되지 않습니다.

Q: SSL 정책에서 FQDN을 사용할 수 있습니까?
A: 현재는 지원되지 않습니다(소프트웨어 버전 6.3.0). FQDN 객체는 AC 정책의 소스 및 대상 네트워크에서만 지원됩니다.

Q: 확인된 FQDN에 대한 정보를 제공할 수 있는 기록 로그가 있습니까? 예를 들어 LINA syslogs와 같습니다.
A: 특정 대상에 대한 FQDN 문제를 해결하려면 system support trace 명령을 사용할 수 있습니다. 추적에는 패킷의 FQDN ID가 표시됩니다. ID를 비교하여 문제를 해결할 수 있습니다. 또한 FQDN dns 확인 활동을 추적하기 위해 Syslog 메시지 746015을 746016 수 있습니다.

Q: 디바이스에서 확인된 IP를 가진 연결 테이블의 FQDN을 로깅합니까?
A: 특정 대상에 대한 FQDN의 문제를 해결하려면 system support trace 명령을 사용할 수 있습니다. 여기서 추적에는 패킷의 FQDN ID가 표시됩니다. ID를 비교하여 문제를 해결할 수 있습니다. 향후 FMC의 이벤트 뷰어에 FQDN 로그를 포함할 계획입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.